Forståelse og forankring af Cybersecurity Awareness

Dylan Møller Jeppesen, Heine Winthereig, Martin Kjærholm Hoeing
IT-Ledelse, Gruppe 16, 2023-05

Specialerapport Cand.IT - IT-ledelse

STUDENTER RAPPORT
AALBORG UNIVERSITY

AALBORG UNIVERSITY
STUDENT REPORT

Cand.IT i IT-ledelse
Aalborg Universitet
http://www.aau.dk

Titel:
Forståelse og forankring
af Cybersecurity Awareness

Tema:
Cybersecurity Awareness

Projektperiode:
Forår 2023

Projektgruppe:
Gruppe 16

Medlemmer:
Heine Winthereig - 20164330
Dylan Møller Jeppesen - 20184694
Martin Kjærholm Hoeing - 20176293

Vejleder:
Kasper Trolle Elmholdt

Antal anslag: 180.504

Antal sider: 75,21

Dato for aflevering:
31. Maj 2023

Abstract

This report investigates the understanding of cybersecurity awareness in the Danish municipality Hjørring Kommune by utilizing Orlikowski and Gash (1994) theory on technological frames. To further understand these technological frames within cybersecurity awareness, the context where the frames are formed and reshaped is analyzed as well. This is done from two analytical angles; an exploration of the cybersecurity awareness culture and awareness maturity, which individually looks at culture regarding cybersecurity awareness and organisational knowledge as well as the attitude towards cybersecurity awareness. This is done to answer the papers following research question:

"What importance does the understanding of cybersecurity awareness have and how does it impact how cybersecurity awareness is ingrained in an organisation?"

This led to a duality of understanding for the workers, as they primarily work on computers, while not acknowledging the importance of their involvement in securing or preventing their organisation from attackers. However, they acknowledge that they lack maturity when it comes to cybersecurity awareness, as relying on the IT-department is a big part of the organizational culture. Furthermore, the paper reveals significant incongruence between the two identified groups' frames. These differences are then further examined by the deeper analysis of culture and maturity within cybersecurity awareness in Hjørring Kommune. Finally, the paper will discuss who is responsible for the level of cybersecurity awareness, the individuals, the organisation or the legislative body. This paper concludes that technological frames supported by a cultural acceptance can be a way of increasing the understanding of cybersecurity awareness of the individual and organisational grasp of the concept.

Forord

Denne rapport er et speciale for udddannelsen Cand.IT i IT-ledelse på Aalborg Universitet. Specialet har haft til formål at undersøge forståelsen af Cybersecurity Awareness og forankringen af dette i en organisation. For at undersøge dette, har specialegruppen samarbejdet med Hjørring Kommune.

Anerkendelser

Vi vil gerne takke Hjørring Kommune for at være behjælpelige i empiriindsamlingen. Det har krævet en stor investering af rescourcer og tid fra deres side, som vi er meget taknemmelige for. Særligt tak til medarbejderne i databeskyttelsesteamet.

En stor tak skal også lyde til projektets vejleder Kasper Trolle Elmholdt, som har bragt vigtig sparring og gode indsigter, som har hjulpet med at facilitere de fund som rapporten har fundet.

Referencemetode

Referencemetoden vi har anvendt er APA formatet. Her bliver forfatterskrevet litteratur i teksten refereret til i formatet (Efternavn, årstal), hvorimod andet litteratur, såsom hjemmesider, virksomheder, nævn, osv. bliver refereret til i formatet (Fulde navn, årstal).
I kildelisten bliver der refereret til litteratur efter følgende format:
Efternavn, initialer. (Udgivelsesdato). Titel. Udgivelseslokation: Udgiver.
I tilfælde hvor kilden er fundet på en hjemmeside, bliver dette noteret i slutningen af referencehenvisningen.

Indhold

1 Introduktion **1**

1.1 Review af eksisterende litteratur . . . 1
1.2 CSA i et forståelsesperspektiv . . . 8
1.3 Forskningsspørgsmål . . . 10
1.4 Introduktion af projektets samarbejdspartner . . . 10

2 Metode **12**

2.1 Dataindsamling . . . 12
2.2 Behandling af empiri . . . 13
2.3 Teoretisk grundlag . . . 15

3 Analyse **19**

3.1 Kortlægning af teknologiske forståelsesrammer omkring CSA . . . 19
3.2 De teknologiske forståelsesrammers kontekst . . . 32
3.3 Konteksten af modenhed omkring CSA . . . 48
3.4 Opsamling af analysen . . . 56

4 Diskussion **58**

4.1 Hvem har ansvaret for CSA? . . . 58
4.2 Udvidelse af teknologiske forståelsesrammer . . . 60
4.3 Hvorfor kontekst i forhold til forståelsesrammer? . . . 61

5 Refleksion **63**

6 Fremtidigt arbejde **64**

7 Konklusion **65**

A Bilag **68**

A.1 Interview - Skolelærer . . . 68
A.2 Interview - Afdelingsleder, handicapområdet . . . 75
A.3 Interview - Demenskonsulent . . . 82
A.4 Interview - Bibliotekar . . . 97
A.5 Interview - Medarbejder 1 i databeskyttelse . . . 107
A.6 Interview - Medarbejder 2 i databeskyttelse (Rekonstruktion) . . . 115
A.7 Interview - Afdelingsleder, sekretariatet (rekonstruktion) . . . 116
A.8 Interviewguide . . . 117
A.9 Ekstraction sheet . . . 118
A.10 Ekstraction sheet - kodning . . . 133

1 | Introduktion

Den eksponentielle stigning af digitale arbejdsgange og hybride arbejdspladser, har gjort at medarbejdere har været tvunget til at hæve deres digitale kompetencer og virksomheder har skulle tilpasse deres platforme til hybride arbejdsgange efter COVID-19 pandemien. Denne digitalisering, der især blev accelereret af pandemien, bragte digitale arbejdsgange til erhverv og stillinger, der ikke tidligere har været omfattet af det helt store niveau af digitalisering.
Dette har ligeledes betydet, at flere og flere mennesker håndterer information digitalt. I en rapport fra World Economic Forum nævnes der at udspredt cyberkriminalitet og cyberusikkerhed som den ottende største risiko for organisationer på globalt plan (*The Global Risks Report 2023 18th Edition*, 2023). Samme rapport fra året før finder, at 95% af alle cybersecurity hændelser kan spores tilbage til menneskelige fejl. Ses dette i sammenhæng med, at alene ransomware angreb er steget med 435%, spiller menneskelige faktorer en større og større rolle i et hastigt voksende trusselslandskab (Foro Económico Mundial. m.fl., 2022).
Dette understreger vigtigheden af begrebet cybersecurity awareness, der netop omhandler dette menneskelige aspekt i forhold til cybersecurity.

Fra et akademisk perspektiv, er det blevet valgt at undersøge dette fænomen, grundet den førnævnte nødvendighed, i kombination med en indsigt, skaffet gennem tidligere litteratur review, at der grundet emnets hastige højnelse i relevans, kan forefindes manglende forskning på området. Et af disse huller er hvordan der er en inkongruens omkring forståelsen af cybersecurity awareness (CSA), hvilket denne rapport vil undersøge nærmere. Målet at undersøge denne forståelse, samt, hvordan der potentielt kan være forskellige niveauer og handlemønstre i forskellige arbejdsmæssige områder i en organisationen, baseret på denne forståelse.

1.1 Review af eksisterende litteratur

For at grave dybere ned i begrebet cybersecurity awareness, er det relevant at undersøge den eksisterende litteratur på området, og på den måde forstå, hvor nye undersøgelser kan føre til værdifuld viden. Vi har valgt at basere dette afsnit på vores litteraturstudie indenfor samme område, der undersøgte, hvordan cybersecurity awareness er konceptualiseret i den eksisterende litteratur (Hoeing m.fl., 2022).
Det følgende afsnit vil indeholde en kondensering af dette litteraturstudie med det formål at give læseren en forståelse af state of the art indenfor cybersecurity awareness forskning og klæde læseren på til den følgende rapport.

Begrebet cybersecurity har udviklet sig en del gennem de 50 år begrebet har eksisteret - fra et mindre projekt inden internettets fødsel til en af de mest kritiske dele af den digitale infrastruktur i verden i dag (Cyber Security Degree, 2023). I dag beskrives cybersecurity og cybersårbarheder som en af de mest kritiske udfordringer globalt (Foro Económico Mundial. m.fl., 2022). Dette sker på baggrund af den enorme mængde data og information, der nu findes digitalt og som håndteres af mennesker. Netop denne menneskelige faktor er kritisk, da det rapporteres, at 95% af cybersecurity hændelser sker på baggrund af menneskelige fejl. I den forbindelse bliver fokus på den menneskelige og organisatoriske del af cybersecurity og cybersecurity awareness ekstremt relevant.
Cybersecurity awareness defineres som en brugers evne til at genkende og undgå aktiviteter, der

truer cybersecurity og agere klogt og ansvarsfuldt til at højne deres cyber safety (Sharif & Ameen, 2020).

Indenfor dette Cybersecurity Awareness begreb findes der i litteraturen to hovedtemaer; *Cybersecurity Awareness trusler* og *organisatoriske opmærksomheder* imod disse trusler. I det følgende afsnit vil disse hovedtemaer udvides yderligere i form af underkategorier, der blev identificeret ud fra den eksisterende litteratur omkring cybersecurity awareness.

Review'et udfolder først de identificerede trusler mod CSA, da det er relevant at kende årsagen til de organisatoriske opmærksomheder først, netop disse trusler.
Herefter udfoldes de organisatoriske opmærksomheder mod disse trusler.

1.1.1 Cybersecurity Awareness trusler

Inden for CSA trusler findes der mange koncepter, hvor *social engineering* (Alsulami m.fl., 2021; Daengsi m.fl., 2022; Pósa & Grossklags, 2022; Trim & Lee, 2019) og *phishing* (Alhashmi m.fl., 2021; Back & Guerette, 2021; Daengsi m.fl., 2022; Trim & Lee, 2019) er de mest undersøgte emner fra litteratursturidet.
Disse er de mest kritiske trusler for en organisation i forhold til data og IT-infrastruktur, hvor mennesket og menneskets interaktion med systemerne, er det svageste led på nuværende tidspunkt. For at forstå de organisatoriske opmærksomheder som organisationer bør have, er det relevant først at forstå de kritiske trusler, organisationer står overfor.

Social Engineering
Social engineering er en manipulationsteknik, hvor ondsindede aktører manipulerer mennesker i den organisation, der ønskes angrebet, til at give adgang til intern data eller værdier. Det kan ses som "menneske-hacking"med det formål at få personer til at give adgang til systemer, lække data eller lignende. Dette kan både ske online eller fysisk (Kaspersky, 2023a). Dette betyder, at social engineering kan være simple angreb, men også langt mere komplekse, hvorfor det er blevet en af de mest udfordrende cybersecurity trusler for organisationer (Pósa & Grossklags, 2022) - dette gælder ikke udelukkende private organisationer, men i lige så høj grad offentlige organisationer.

Social engineering kan ses som en form for informationsopsamling for de ondsindede aktører, hvor præmissen er, at, hvis det menneskelige aspekt angribes, kan denne private information opsamles. En måde, hvorpå dette kan ske er eksempelvis ved, at ondsindede aktører udgiver sig for at være en kollega, chef eller anden person, den angrebede part har et forhold til. Dette betyder også, at social engineering ofte er blandet sammen med andre former for angreb, hvor phishing er den mest prominente på nuværende tidspunkt (Hoeing m.fl., 2022; Pósa & Grossklags, 2022).

Social engineering er altså angreb mod det menneskelige aspekt, hvorfor IT-sikkerhedssystemer ikke kan forsvare en organisation mod denne form for angreb. Da social engineering samtidig kan foregå på meget komplekse og snedige måder fra angribernes side, bliver det til en af de mest udfordrende cybersecurity trusler for organisationer (Pósa & Grossklags, 2022) Da sikkerhedssystemer ikke kan forsvare mod denne type af trusler, er CSA det bedste forsvar. Der kræves derfor en tilstedeværelse af CSA i organisationer:

> *"A number of research studies highlight that all users or employees need to be aware of important social engineering attack vectors because technical measures (such as email filtering) are not sufficient for managing these events"*
> (Pósa & Grossklags, 2022)

Den bedste måde, hvorpå organisationer kan beskytte sig mod denne form for trusler er altså med fokus på cybersecurity awareness og opbygning af forsvaret indenfor det menneskelige aspekt.

Phishing
Phishing trusler er en form for social engineering angreb, hvor formålet er at tilegne sig adgang til systemer eller sensitive informationer. Herefter kan det oprindelige mål med angrebet udføres, eksempelvis ransomware-angreb, hvor filer låses og der kræves en løsesum for at låse dem op igen. Phishing er altså en trussel, der har til formål at snyde brugere af systemer til at give de ondsindede aktører adgang til systemer eller data, der senere anvendes ulovligt (Merriam-Webster, 2023)
Førhen blev langt de fleste af disse former for angreb fanget i sikkerhedssystemer, men disse angreb er blevet langt mere målrettede - eksempelvis i form af spear-phishing (Kaspersky, 2023b) - og derfor sværere for sikkerhedssystemer at genkende (Daengsi m.fl., 2022).

> "Previously, cyber-attacks were normally indiscriminate without a specific target. However, current cyber-attacks have transformed into goal oriented attacks on designated targets"
> (Daengsi m.fl., 2022)

Ligesom ved social engineering, er det derfor modtagerne i organisationerne, der er det bedste forsvar mod disse trusler, da det bliver umuligt for sikkerhedssystemerne at opfange alle disse angreb. Her er der altså igen stærke beviser for, at CSA er yderst relevant og nødvendigt (Alhashmi m.fl., 2021; Back & Guerette, 2021; Daengsi m.fl., 2022).

Phishing-angreb bliver oftest tænkt som angreb over e-mail, men udbredelsen af sociale medier, online-møde systemer og lignende netværk, betyder også, at phishing angreb kan foregå disse steder (Hoeing m.fl., 2022).

> *"It can be argued that cyber security awareness training needs to take into account online activities such as blogging, instant messaging and social networking that employees engage in while at work"*
> (Trim & Lee, 2019)

Relevansen af, at anse phishing som en reel trussel, ses især også ved de store konsekvenser ved denne type af angreb. 90% af alle cyberangreb er phishing-angreb og omkostningerne for organisationer på baggrund af disse angreb, er på verdensplan estimeret til over en billion dollars (Alhashmi m.fl., 2021). Sættes dette i kontekst af, hvor effektive disse angreb er - en rapport om data breaches fra den amerikanske teleudbyder Verizon, nævnte at 30% af phishing emails var læst af ofre og 12% af de ofre klikkede på linket eller vedhæftede filer - bliver organisationer nødt til at tænke i det menneskelige aspekt i et forsvar mod disse (Hoeing m.fl., 2022).

1.1.2 Organisatoriske opmærksomheder

Litteraturen beskriver som forsvar til de tidligere beskrevne trusler flere fokuspunkter som organisationer kan være opmærksomme på. Disse opmærksomheder kommer til syne i seks koncepter; *Adfærd* (Alhashmi m.fl., 2021; Alhuwail m.fl., 2021; Alqahtani, 2022; Alsulami m.fl., 2021; Back & Guerette, 2021; Barlow m.fl., 2013; Canham m.fl., 2022; Jensen m.fl., 2019; Sharif & Ameen, 2020; Trim & Lee, 2019),

IT Governance (Alhuwail m.fl., 2021; Barlow m.fl., 2013; Sharif & Ameen, 2020; Trim & Lee, 2019),

Strategi (Alhashmi m.fl., 2021; Alhuwail m.fl., 2021; Back & Guerette, 2021; Daengsi m.fl., 2022; Jensen m.fl., 2019; Li m.fl., 2021; Pósa & Grossklags, 2022; Sharif & Ameen, 2020; Shojaifar & Fricker, 2020; Wang m.fl., 2022),

Træning (Alhashmi m.fl., 2021; Alhuwail m.fl., 2021; Alsulami m.fl., 2021; Alzahrani, 2021; Arain m.fl., 2019; Barlow m.fl., 2013; Canham m.fl., 2022; Hepp m.fl., 2018; Sharif & Ameen, 2020; Trim & Lee, 2019; Wang m.fl., 2022),

Kultur (Abawajy, 2014; Li m.fl., 2021; Trim & Lee, 2019),

Incitamentstrukturer (Alzahrani, 2021; Barlow m.fl., 2013; Canham m.fl., 2022; Jensen m.fl., 2019; Trim & Lee, 2019).

Adfærd
Cybersecurity awareness og en skabelse af denne i en organisation, er en ændring af adfærd hos brugerne i organisationen. Målet med CSA er altså, at ændre adfærden hos brugerne til en mere sikker og compliant adfærd. At skabe adfærdsændringer kan dog være en stor udfordring, da mennesker er vanedyr.
De fleste mennesker er, ifølge den eksisterende litteratur, udmærket klar over, at cybersecurity awareness er nødvendigt i deres arbejdshverdag - også selvom det ikke nødvendigvis er en del af deres kerneopgaver. Det viser sig dog, at CSA bliver nedprioriteret i forhold til disse kerneopgaver (Barlow m.fl., 2013).

Litteraturen viser yderligere grunde til, at CSA bliver nedprioriteret af medarbejdere i hverdagen. Dette kan blandt andet være, hvis medarbejdere ikke mener, at den/de opgaver, der udføres ikke er af kritisk karakter for organisationen (Barlow m.fl., 2013). På den måde rationaliserer medarbejderen bruddet på sikkerhedsforanstaltninger med en risikovurdering af, hvad der kan gå galt, hvis et brud skulle finde sted i arbejdsgangen. Denne vurdering er dog ofte fejlagtig.

Et andet eksempel på bevidst usikker adfærd, er hvis brugere overlagt bryder sikkerhedsforanstaltninger, fordi de mener, det er nødvendigt for at udføre deres arbejde. Her rationaliserer brugeren deres usikre adfærd med en følelse af nødvendighed, for at kunne udføre deres opgaver.
Træning eller oplysning i CSA bliver derfor ikke udelukkende vedrørende politikker, praksisser og lignende, men også ændring af adfærd.

> *"To reduce the possibility of a data breach, senior management need to increase threat awareness through the development of an awareness programme by relating an individual's knowledge and attitude to their change in behaviour"*
> (Trim & Lee, 2019)

De forskellige rationaler for usikker adfærd beskrevet her, viser også, hvor forskellig adfærden hos medarbejdere kan være. At arbejde med en sådan kollektiv adfærdsændring på et organisatorisk niveau, kan derfor være en stor udfordring.

> *"...security awareness programme may be well thought through but deficient in terms of getting people to act responsibly. This is due to a number of factors including personal characteristics, cultural differences, rewards and punishments, and media-framed messages"*
> (Trim & Lee, 2019)

Da mennesker er forskellige, kan det ligeledes betyde, at der kræves forskellige metoder til forskellige brugere i forhold til at skabe denne adfærdsændring. Litteraturen viser dog, at dette er essentielt for at lykkes (Hoeing m.fl., 2022).

IT Governance
Et effektivt organisatorisk værktøj mod de CSA trusler, litteraturen viser, kan være IT Governance, især cybersecurity politikker. Dette bliver defineret som et rammeværk for beslutningsrettigheder og ansvar til at tilskynde en ønskelig adfærd ved brugen af IT:

> *"We define IT governance as specifying the framework for decision rights and accountabilities to encourage desirable behavior in the use of IT"*
> (Weill, 2004)

Denne definition har igen fokus på adfærd hos medarbejderne. Yderligere beskriver Weill (2004), at denne ønskede adfærd skal være i forlængelse af organisationens overordnede strategi, kultur, værdier og lignende. Litteraturen viser dog, at især politikker indenfor cybersecurity er særdeles fremtrædende:

> *"Research has shown that the most important issues and factors that affect security awareness among end-users are as follow: Information Security Policy..."*
> (Sharif & Ameen, 2020)

Litteraturen viser, at organisationer i høj grad beror sig på tekniske cybersecurity forsvar, men indikerer også, at disse forsvar i lige så høj grad bør have fokus på den ikke-tekniske del - altså det menneskelige aspekt (Sharif & Ameen, 2020). I den forbindelse viser litteraturen, at noget så simpelt som, at medarbejderne kender til organisationens sikkerhedspolitikker, kan være et væsentligt forsvar:

> *"The results show that when employees are aware of their company's information security policy and procedures, they are more competent to manage cybersecurity tasks than those who are not aware of their companies' cybersecurity policies"*
> (Li m.fl., 2021)

Dog viser litteraturen, at disse politikker - og information omkring deres eksistens - ikke er tilstrækkeligt som CSA forsvar. Barlow m.fl. (2013) definerer således tre årsager til, at medarbejdere bryder organisationens politikker:

- Defense of necessity - En medarbejder mener, at et brud på sikkerhedspolitikker er nødvendigt for, at arbejdet kan udføres.
- Denial of injury - En medarbejder mener, at ingen vil komme til skade ved et brud på sikkerhedspolitikker.
- Metaphor of the ledger - En medarbejder mener, at vedkommende har gjort nok gode gerninger til at tillade sig at bryde sikkerhedspolitikker

Yderligere beskriver Sharif og Ameen (2020), at nogle medarbejdere simpelthen også bare kan være ligeglade med en organisations sikkerhedspolitkker. Dette viser vigtigheden af, at disse politikker er til stede i en organisation, og at der informeres omkring dem, men også, at det er adfærd, der arbejdes med, hvilket er en kæmpe udfordring.

Strategi og træning
Litteraturen omkring strategi omhandler hovedsageligt strategi om træning. Disse to underkategorier er derfor samlet i dette afsnit.

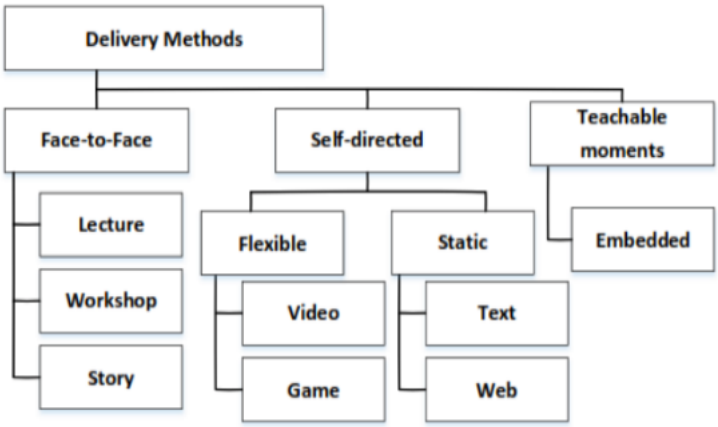
Litteraturen viser tydeligt, at CSA initiativer har en effekt på CSA i en organisation - dog er dette kun tilfældet, hvis initiativerne er en del af en konkret og velgennemtænkt strategi (Jensen m.fl., 2019). Da litteraturen og truslerne mod organisationer viser, at tekniske løsninger ikke længere er tilstrækkelige, er der bred enighed i litteraturen omkring, at uddannelse af medarbejdere i CSA er kritisk (Pósa & Grossklags, 2022). I den forbindelse viser undersøgelser, at dette har en positiv effekt på en organisations CSA evner og også generelle cybersecurity:

> *"Past research has demonstrated that SETA (Security Education, Training and Awareness) initiatives can have a significant effect on improving IT security cap- abilities within organisations"*
> (Jensen m.fl., 2019)

Litteraturen beskriver, at strategier omkring CSA hovedsageligt sker ved at gennemføre træninger i cybersecurity (Pósa & Grossklags, 2022). Der er i litteraturen bred enighed omkring, at strategien og træninger skal opdateres og være kontinuerlige, da CSA truslerne kan udvikle sig gevaldigt over tid (Alqahtani, 2022). Samtidig bør disse træninger tilrettelægges på forskellige måder i forhold til, hvem der modtager træningen.

> *"Therefore, for the cybersecurity intervention program to be effective and successful in reducing human factor related security issues, appropriate delivery methods for cybersecurity awareness training intervention programs should be used"*
> (Alhashmi m.fl., 2021)

Dette betyder også, at valg af træningsmetoder og værktøjer i strategien er kritiske for succesen af CSA. Som nævnt tidligere, kræver ændringen af adfærd forskellige metoder, hvilket skal tages i betragtning i den overordnede strategi også. Ofte er det fordelagtigt at anvende flere end én metode til træningen, for at lykkedes. En oversigt over de mest hyppige træningsmetoder, der går igen i litteraturen kan ses i figur 1.1.



Figur 1.1: De mest hyppige træningsmetoder (Alhashmi m.fl., 2021)

Kultur
I forlængelse af IT Governance og adfærds-konceptet, beskriver litteraturen, at en kultur omkring CSA kan være løsningen (Trim & Lee, 2019).

> *"Senior management need to promote an in-house security culture... ...to ensure that they introduce and main- tain appropriate security measures"*
> (Trim & Lee, 2019)

Ved at skabe en bevidsthed omkring cybersecurity, der er indlejret i organisationskulturen, gøres CSA til en del af hverdagen for brugerne. Dette kan eksempelvis være særdeles fordelagtigt for at imødekomme den forskellighed, der vil være mellem brugere (Trim & Lee, 2019).

Yderligere vil udviklingen af en kultur, der promoverer en sikker adfærd blandt medarbejdere, ifølge litteraturen føre til en kontinuerlig udviklende proces, hvor medarbejdere også lærer af hindanden og udvikler sig individuelt.

> *"Managers should also know how they can stimulate their staff to embrace a cyber security culture and gain additional knowledge and skills through a continual process of self development"*
> (Trim & Lee, 2019)

Samtidig opfordrer en kultur til en bestemt adfærd, hvilket i sidste ende er målet med CSA.

Incitamentstrukturer
Litteraturen viser, at en sikker adfærd og skabelsen af denne er det endelige mål med CSA. Dette betyder, at organisationer kan opsætte incitamentstrukturer, for at tilskynde en sådan adfærd. Dette gælder også for at deltage i træninger, overholde politikker omkring CSA og lignende (Jensen m.fl., 2019).
Her kan det være nødvendigt at skabe en klarhed omkring konsekvenserne ved CSA trusler og gevinsten ved CSA. Yderligere beskrives det, hvordan en alignment i forståelsen af det kritiske niveau af truslerne, kan øge motivationen for CSA gevaldigt, således, at medarbejdernes opfattelse af en trussel har stor betydning på, hvorvidt arbejdet med CSA lykkes.

> *"We argue that when SETA initiatives invoke threat susceptibility, individuals likely evaluate these claims against their existing attitudes towards the threat. If individuals' attitudes are congruent with susceptibility claims, the SETA initiative will be more likely to succeed in motivating behaviour change"*
> (Jensen m.fl., 2019)

I den forbindelse beskriver litteraturen, at skrækhistorier og konsekvenserne ved et eventuelt angreb ofte virker som et fordelagtigt incitament for medarbejdere (Jensen m.fl., 2019).

1.2 CSA i et forståelsesperspektiv

Review'et af den eksisterende litteratur omkring cybersecurity awareness tegner et billede af nogle begreber og forskningsområder, der går igen gennem litteraturen. I vores litteraturstudie, som review'et er en kondensering af, kaldte vi disse begreber og forskningsområder for *CSA trusler* og *organisatoriske opmærksomheder* mod disse.
Review'et gør det klart, at truslerne er reelle, har enorme konsekvenser for de udsatte organisationer, og at de ondsindede aktører bliver stadig mere udspekulerede og sofistikerede i deres metoder. Cybersecurity systemer bliver ligeledes mere sofistikerede og i den forbindelse bliver det menneskelige aspekt i højere grad målet for angrebene. Dette berettiger i den grad eksistensen af begrebet cybersecurity awareness, der skal udvikle det menneskelige forsvar, og forskning heri.

Den nuværende litteratur indenfor CSA har hovedsageligt fokus på, at det menneskelige aspekt styrkes ved at træne og oplære medarbejdere i cybersecurity. Litteraturen på området bliver således næsten udelukkende undersøgelser af effekten af forskellige måder, hvorpå en sådan træning kan tilrettelægges, planlægges og udføres.
Vi mener, at dette ikke udforsker CSA-begrebet tilstrækkeligt. Et gennemgående koncept gennem litteraturreview'et er adfærd blandt medarbejdere og, at CSA er en ændring af denne. Vi argumenterer for, at adfærd er et så unikt og subjektivt fænomen, at undersøgelse af træning og træningsmetoder ikke er tilstrækkeligt for at forstå medarbejderes adfærd og, hvordan denne påvirkes til en ændring mod en sikker adfærd i forhold til CSA.
Subjektiviteten af adfærd fordrer i stedet en undersøgelse af, hvordan den enkelte medarbejder oplever, skaber mening af, og forstår begrebet CSA. Litteraturen beskriver, hvordan det menneskelige aspekt ved cybersecurity er kritisk - vi argumenterer for, at det er nødvendigt at forstå mennesket og dets forståelse af begrebet, for at kunne arbejde med dette menneskelige aspekt.

I den forbindelse, præsenteres Orlikowski og Gash (1994) teori om teknologiske forståelsesrammer. Denne teori vil anvendes som den overordnede struktur i denne opgave med det formål at undersøge, hvilken betydning forståelser af begrebet har, for arbejdet med CSA.
Orlikowski og Gash (1994) baserer deres teori omkring teknologiske forståelsesrammer på tidligere teori omkring sociale og kognitive aspekter i forhold til udvikling og implementering af ny IT. Orlikowski og Gash (1994) bygger videre på disse teorier og argumenterer for, at en socio-kognitiv tilgang til IT er nødvendig ved udvikling og implementering af nye teknologier:

> *"We argue that an understanding of people's interpretations of a technology is critical to understanding their interactions with it. To interact with technology, people have to make sense of it; and in this sense-making process, they develop particular assumptions, expectations, and knowledge of the technology, which then serve to shape subsequent actions toward it"* (Orlikowski & Gash, 1994, s. 175)

Orlikowski og Gash (1994) argumenterer for at individers kognitive strukturer også udvider sig til grupper og hele organisationer, der bliver til rammer til forståelse - eller forståelsesrammer. Rammer i denne sammenhæng, skal forstås som *"definitioner af organisationel virkelighed, der fungerer som fundament for forståelse og handling"* (Orlikowski & Gash, 1994). Disse rammer indeholder antagelser, viden, forventninger, metaforer, fortællinger, og lignende. De er fleksible i deres struktur og indhold, og skal ses mere som net, der er flettet sammen, end lineære strukturer.

Individer kan have individuelle forståelsesrammer, men samtidig også være del af en gruppe, der deler nogle antagelser, viden, forventninger eller lignende, og dermed har en fælles forståelsesramme. Det ses dog, at en gruppes forståelsesramme har stærk effekt på de enkelte individers forståelsesramme også.

Teknologiske forståelsesrammer omhandler forståelser omkring teknologiske artefakter, hvilket kan komme til syne som viden omkring den specifikke teknologi eller viden omkring anvendelsen af teknologien i en specifik situation. Orlikowski og Gash (1994) argumenterer for, at forskellige forståelsesrammer blandt forskellige grupper i en organisation kan skabe problemer i forbindelse med udvikling, implementering eller anvendelse af IT. Denne forskellighed kalder de inkongruens. Formålet med at analysere teknologiske forståelsesrammer i en organisation, er derfor at skabe et billede over de forskellige forståelsesrammer, der eksisterer og forsøge at skabe kongruens blandt disse.
Kongruens er i denne sammenhæng ikke at skabe identiske forståelsesrammer, men at skabe en fælles struktur eller indhold for rammerne - altså at skabe signifikant konsensus omkring forståelsen af IT, information eller lignende. Dette kan eksempelvis være forståelsen for anvendelsen af et system i organisationen eller hvor tit systemet skal vedligeholdes.

Det er værd at bemærke, at Orlikowski og Gash (1994) teknologiske forståelsesrammer drejer sig om et specifikt IT-system, såsom implementeringen af et IT-system. I dette projekt søger vi at undersøge cybersecurity awareness og ikke et specifikt IT-system. Vi argumenterer alligevel for, at konceptet om forståelsesrammer er relevant i en CSA sammenhæng, da den eksisterende litteratur viser, at det menneskelige aspekt bør undersøges nærmere. Orlikowski og Gash (1994) argumenterer for, at for at forstå brugeres interaktion med IT, er det nødvendigt at forstå deres fortolkning og forståelse af denne IT. Denne argumentation mener vi også gælder ved cybersecurity awareness, hvorfor vi tager udgangspunkt i denne teori. Yderligere mener vi, at der mangler undersøgelser indenfor dette område i CSA-forskningen, hvorfor vi håber at bidrage med en ny vinkel.

Orlikowski og Gash (1994) danner altså udgangspunkt for undersøgelsen i denne rapport. Vi mener dog, at for at forstå individer og gruppers forståelse og fortolkning af IT, er det ligeledes nødvendigt at forstå den kultur, de befinder sig i. Analysen i denne opgave vil derfor ligeledes indeholde en analyse af denne kultur i form af en domæneanalyse, for at undersøge den kontekst som forståelserne bliver skabt og formet i.
Yderligere findes det relevant at undersøge, hvordan de tidligere indetificerede organisatoriske opmærksomheder fra litteraturstudiet kan påvirke de kortlagte forståelsesrammer. For at forsøge at indkapsulere flere af de organisatoriske opmærksomheder fra den eksisterende litteratur, analyseres den organisatoriske modenhed i forhold til CSA.

Dette findes relevant for at undersøge, hvorvidt denne organisatoriske modenhed også har indflydelse på forståelsesrammerne og i sidste ende på adfærden i forhold til CSA.

Dette leder videre til forskningsspørgsmålet i denne undersøgelse, som vil præsenteres i følgende afsnit.

1.3 Forskningsspørgsmål

Som tidligere beskrevet er formålet med denne rapport at undersøge de teknologiske forståelsesrammer i forhold til CSA i Hjørring Kommune. Dette gøres for at undersøge, hvorvidt forståelser af begrebet har indflydelse på, hvordan CSA forankres i en organisation. Dette vil gøres ud fra følgende forskningsspørgsmål:

Hvilken betydning har forståelse for cybersecurity awareness på, hvordan cybersecurity awareness forankres i en organisation?

Forskningsspørgsmålet vil forsøges besvaret ud fra en empirisk undersøgelse af Hjørring Kommune. I det følgende afsnit vil følge en præsentation af Hjørring Kommune som organisation og samarbejdspartner i dette projekt.

1.4 Introduktion af projektets samarbejdspartner

Projektet er udarbejdet i samarbejde med Hjørring Kommune, som har stillet interviewpersoner til rådighed, samt været behjælpelig med at give indsigter i organisationens arbejde med CSA. Projektgruppen valgte at samarbejde med Hjørring Kommune, da de allerede har anerkendt, at en investering i cybersecurity awareness er nødvendig, da de har et dedikeret databeskyttelses team. Det unikke ved at samarbejde med en stor offentlig organisation er, at deres faglige felt spreder sig bredt, for at kunne yde borgerne en god service.
Som offentlig organisation, med en pligt til at forsørge deres borgere, håndterer Hjørring Kommune meget kritisk borgerdata. Hjørring Kommune er derfor en godt eksempel på en organisation, der udsættes for aggresiv digital acceleration på baggrund af denne nødvendighed. Der følger derfor et stort arbejde med at følge med denne udvikling, især i form af digitale arbejdsgange og sikkerhed forbundet med disse.

Hjørring kommune er en stor organisation, med omkring 6000 medarbejdere, som yder service for over 60.000 borgere. Disse services dækker over alt fra biblioteker, uddannelsesområdet, til ældreplejen med flere.
Hjørring Kommune er dermed den andenstørste kommune i Nordjylland.

Projektets primære kontakter ved Hjørring Kommune har været afdelingen for databeskyttelse, som er underlagt IT-afdelingen. Her sidder der til dagligt to fuldtidsansatte, samt én deltidsansat, som har til ansvar at styrke den kommunale indsats på sikkerhedsområdet. Deres fokusområder er primært at sikre overholdelse af GDPR-lovgivningen, samt awareness på cybersecurity området. I de indledende møder med Hjørring Kommune bliver det tydeliggjort, at de er meget tidligt i deres omgang med cybersecurity awareness. De har valgt at tage en mere passiv og reaktiv

tilgang, hvor medarbejdere i kommunen selv henvender sig til databeskyttelsesteamet, hvis de oplever udfordringer med cybersecurity. Udfordringen for databeskyttelsesteamet er på nuværende tidspunkt at kunne række ud til de resterende medarbejdere i organisationen og være mere aktive i forebyggelsen af sikkerhedsbrud.

Interviewpersonerne fra organisationen er fra forskellige områder, som f.eks. uddannelsesområdet, ældreområdet, biblioteket, samt medarbejdere fra databeskyttelsesteamet. Disse interviewpersoner blev udvalgt på baggrund af en forespørgsel om at få så bred en repræsentation af organisationen som muligt, hvor interviewpersonerne kommer med en variation i deres viden af cybersecurity.

2 | Metode

Dette afsnit præsenterer, fremgangsmåden anvendt til dataindsamling, behandlingen af empirien, samt præsentation af de teorier, der anvendes til at belyse konteksten, hvori forståelsesrammerne opstår.

2.1 Dataindsamling

Dataindsamalingen i denne rapport er indsamlet ved kvalitative, semistrukturerede interviews. Denne tilgang forsøger at forstå frem for at måle, som Bryman (2012) beskriver: "(...) a research strategy that usually emphasizes words rather than quantification in the collection and analysis of data". Dette perspektiv resonerer med projektets forskningsspørgsmål og fokusset som ligger i forståelsen af individers forståelse af CSA.

I forbindelse med disse semistrukturerede interviews, blev en interviewguide udarbejdet. Denne interviewguide har til formål at skabe en struktur for interviewet samt sikre et flow og fleksibilitet, der giver interviewpersonerne god mulighed for at komme med deres udtalelser omkring CSA. En fordel ved semistrukturerede interviews er dog, at der er en frihed både for respondenten og interviweren til at bevæge sig væk fra denne interviewguide, hvis findes relevant under interviewet.
Netop denne frihed finder vi fordelagtig i det induktive, kvalitative arbejde med forståelser, hvorfor denne dataindsamlingsmetode er valgt.
Udarbejdelsen af interviewguiden beskrives i næste afsnit og den fulde interviewguide kan ses i bilag A.8.

2.1.1 Interviewguide

Inden interviewene blev afholdt hos Hjørring Kommune blev der, som tidligere nævnt, udarbejdet en interviewguide, der havde til formål at styre retningen af interviewene. Som beskrevet havde denne guide til formål at sikre fuld udnyttelse af den tid, der var til rådighed med respondenterne og sikre, at dialogen forholdte sig relevant, men hvor der stadig var frihed for interviewpersonerne til at udtrykke sig frit og åbent. Effektiviteten og tidsrammen for interviewene var vigtigt for empiriindsamlingen, for bedst muligt at respektere samarbejdsvirksomhedens tid. Da der var sat forudbestemt tid af med hver interviewperson, fungerede interviewguiden ligeledes som tidsstruktur for interviewene. Formålet med udarbejdelsen af interviewguiden, er derfor også at skabe en genskabelig fremgangsmåde, der ligeledes sikrer en validitet og reliabilitet af empirien.

For at få den bredeste mulige empiri ville interviewpersoner fra forskellige grene af virksomheden være essentielt, hvilket var tilfældet, da der var interviews med projektledere, en skolelærer, en bibliotekar, en demenskonsulent og medlemmer af databeskyttelsesteamet, hvilket ville gøre undersøgelsen mere repræsentativ for organisationen.

Indholdet i interviewguiden blev udarbejdet ud fra, hvad samarbejdsvirksomheden ønskede at få ud af samarbejdet, sammen med det akademiske bidrag projektgruppen ønskede at undersøge.

Interviewguiden blev designet efter at interviewpersonerne mødte op uden at være forudkonditioneret, så man fik deres ufiltrerede og reelle mening om CSA, hvor de efterfølgende i løbet af

interiewet ville få mere viden indenfor emnet, og se hvordan deres forståelse udviklede sig i løbet af interviewet, samt hvordan nogle af deres holdninger, perspektiver og/eller fremtidige handlinger potentielt kunne ændre sig baseret på de nye indsigter. Dette vil også have formålet at gøre interviewpersonerne mere parate til at ændre deres initielle holdninger og afmystificere emnet. Da formålet med undersøgelsen er at undersøge respondenternes forståelser omkring CSA, fandt vi netop denne fravalgte forudkonditionering ekstremt vigtig. Dette mener vi på bedste vis ville give os det mest reelle indblik i deres forståelse af CSA på nuværende tidspunkt.

Første skridt i interviewet omhandler, at de præsenterer deres stilling og hvilke tre ord de associerer med CSA, efter de har fået forklaret hvad interviewets fokus er. Interviewets hovedfokus er at undersøge interviewpersonernes forståelse af CSA, hvilket betyder at de ikke vil blive rettet på undervejs, og at der ikke findes forkerte svar.

Andet skridt er at undersøge deres kendskab til cybersecurity. Dette zoom ud har til formål at undersøge interviewpersonens relation til cybersecurity generelt, for senere at zoome ind på deres specifikke forståelse af CSA. Efter der er zoomet ind på deres forståelse af CSA, og interviewpersonen har tilkendegivet deres forståelse af CSA, bliver der undersøgt hvad deres opfattelse af at være aware i denne kontekst er.

Tredje skridt undersøger derefter interviewpersonens indblik i organisationens forståelse af CSA og om, hvorvidt der er forskellige forståelser af termet på tværs af organisationen. Dette har til formål at give et indblik i om der faktisk er inkongruens i forbindelse med forståelsen af termet, ud fra deres synspunkt.

Fjerde skridt undersøger interviewpersonens subjektive holdning i forhold til vigtigheden af både cybersecurity og CSA, samt om de mener, det fylder meget i deres arbejdsdage. Dette skridt har til formål at få interviewpersonerne til at fortælle om deres praktiske holdninger til CSA, samt en anden vinkel på deres subjektive opfattelse af vigtigheden af CSA, for igen at undersøge, hvor stor en eventuel inkongruens der er i organisationen.

Femte skridt har til formål at undersøge deres praktiske viden om, hvordan dataen i virksomheden bliver opbevaret, håndteret og sendt i arbejdsdagen. Dette giver et indblik i den praktiske viden i forbindelse med, hvordan de bearbejder sensitiv data, og hvorvidt deres kendskab til nogle af de både tekniske og teoretisk bedste handlinger indenfor både cybersecurity og CSA. Dette fortæller også, om interviewpersonerne og deres kollegaers opfattelse af vigtigheden og dataens subjektive værdi hos de personer.

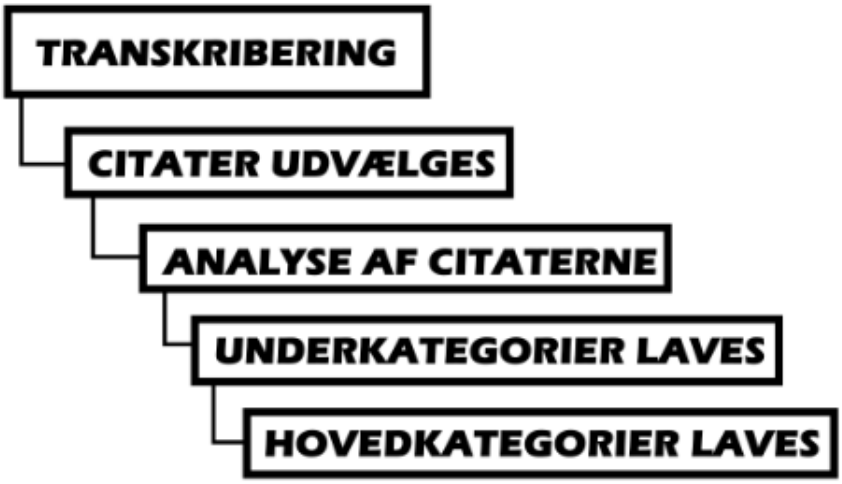
De sidste skridt undersøger om interviewpersonernes perspektiv har ændret sig efter interviewet, og om interviewet har ændret deres synspunkt på cybersecurity og specielt CSA. Her bliver de bedt om at skrive tre ord ned om deres opdaterede syn af CSA. Dette undersøger om der er en ny opfattelse af begrebet og om vigtigheden af emnet har ændret sig subjektivt hos interviewpersonerne.

2.2 Behandling af empiri

I dette afsnit vil der blive beskrevet, hvilke metoder der bliver anvendt til at behandle empirien fra de afholdte interviews. Hvert interview blev efterfølgende transskriberet. Denne transkribering vil derefter danne grundlag for udvalgte citater som vil blive selektivt kodet.
Inden selve udvælgelsen fandt sted, blev der lavet en udvælgelsesguide. Herefter læste hvert

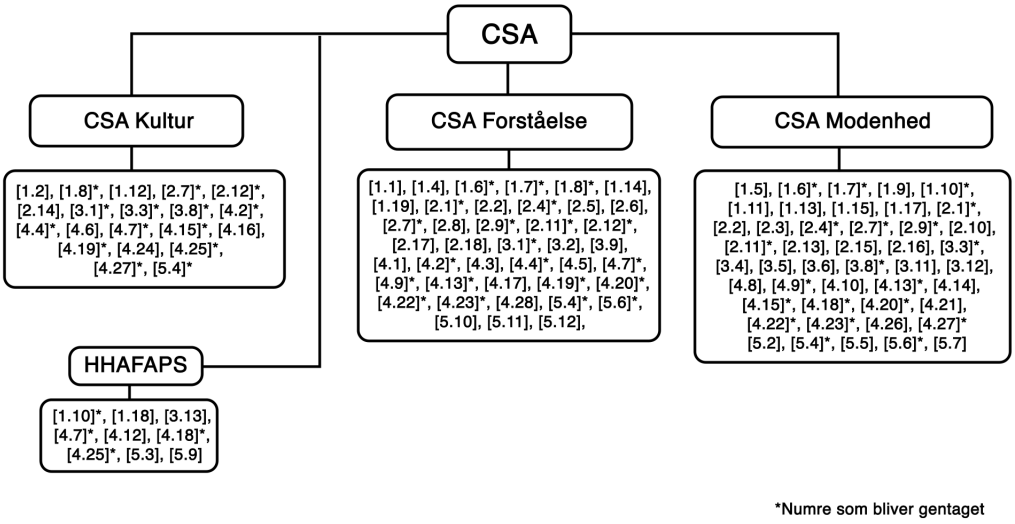
gruppemedlem alle interviews igennem og udvalgte citater. Herefter blev de udvalgte citater drøftet i gruppen og herefter kodet. Denne analyse og kodning af de udvalgte citater skete med udgangspunkt i Wolfswinkel m.fl. (2013) induktive metode. Det er vigtigt at nævne, at interviewene i bilag A.6 og bilag A.7 havde en fejl i lydoptagelsen, hvorfor disse ikke var mulige at transkribere, men i stedet er blevet rekonstrueret.

Wolfswinkel m.fl. (2013) metode indeholder kodning af empirien i tre stadier; open, axial og selektiv kodning. Ud fra Wolfswinkel m.fl. (2013) artikel er deres beskrivelse designet til litteraturstudier, hvor dette projekt tog udgangspunkt i metoden til kodning af interviewene. Vi mener, metoden er relevant i denne sammenhæng også, da fokus er på den kvalitative metode og undersøgelsen omhandler forståelser omkring et begreb.
Åben kodning omhandler at udvælge uddrag fra litteraturen, der har betydning for forskningsspørgsmålet. I dette projekt skal transskriberingerne ses som "den udvalgte litteratur", hvorfor der vil udvælges herfra. Dette resulterer i navngivelsen og dannelsen af kategorier.
Axial kodning omhandler de overordnede kategorier, som er identificeret gennem den åbne kodning, hvorefter disse forskellige katergorier bliver sat op imod hinanden og der bliver udviklet underkategorier.
Selektiv kodning går ud på at skabe hovedkategorier ud fra de to tidligere skridt og identificere relationer mellem disse kategorier. En visualisering af denne metode kan ses i figur 2.1.



Figur 2.1: Behandling af data - egen tilvirkning

Hovedkategorierne vil blive holdt op imod forskningsspørgsmålet for at sikre, at der er en enighed om betydelsen af diverse kategorier, samt forståelsen af dem. Yderligere vil den selektive kodning undersøge relationerne mellem kategorierne, hvilket ligeledes er relevant i vores undersøgelse, for at undersøge om kulturelle og modenhedsmæssige aspekter påvirker konteksten for forståelsen.



Figur 2.2: Den færdige kodeproces - egen tilvirkning

Den endelige kodning fra kodningsprocessen er illustreret i figur 2.2, hvor hovedkategorien er CSA. Kodningen fandt frem til fire hovedkategorier; CSA Kultur, CSA Forståelse, CSA Modenhed og HHAFAPS (Hvem har ansvaret for awareness på samfundsmæssigt plan). Hvert kodningsnummer refererer til specifikke citater som kan ses i, hvad vi kaldte et "extraction sheet"i A.9. Disse kodninger er fundamentet for analysen, hvor de mest relevante kodninger blev udvalgt og anvendt til at belyse argumenter fra empirien.

2.3 Teoretisk grundlag

Dette afsnit vil introducere læseren til den teori, der anvendes i analysen af den indsamlede empiri. Som beskrevet tidligere, er formålet med dette speciale at undersøge forskellige forståelser af CSA. Derfor er denne teori introduceret tidligere. Dog har kultur en markant indflydelse på forståelse og fortolkning, hvorfor dette afsnit vil introducere domæneanalyse, der anvendes til at undersøge dette kulturelle aspekt, stadig med teknologiske forståelsesrammer in mente.
Yderligere vil følge en præsentation af teori omkring organisatorisk modenhed vedrørende CSA. Denne teoretiske vinkel har til formål at belyse konteksten for det nuværende kendskab og attitude i forhold til forståelse af CSA.

2.3.1 Den kulturelle kontekst for forståelsesrammer

Som beskrevet, vil analysen forsøge at undersøge kulturen omkring cybersecurity awareness i Hjørring Kommune, for at forstå denne kultur og på den måde give klarhed over, hvordan der kan forankres et større fokus omkring CSA i denne. Måden hvorpå dette vil undersøges i denne rapport, er ved en etnografisk domæneanalyse. En etnografisk analyse, er en undersøgelse af delene af en kultur og sammenhængende mellem disse dele, som de er beskrevet af respondenterne. Dette er ligeledes i tråd med projektets induktive tilgang. En domæneanalyse er oftest den første del af en

større etnografisk analyse og anvendes til at identificere de kulturelle domæner - dele - af kulturen. I denne rapport vil en analyse af de kulturelle domæner hos Hjørring Kommune undersøges for at forstå kulturen af cybersecurity awareness og hvordan denne skaber kontekst for skabelsen af forståelser.

Et domæne defineres som en symbolsk kategori, der indeholder andre kategorier (J. P. Spradley, 1979). En kategori er i denne sammenhæng en liste af ting, som behandles som havende tilsvarende egenskaber - eksempelvis kan alle træer samles i kategorien 'træer', men kan også skelnes fra hinanden eksempelvis ved deres sort. En symbolsk kategori fungerer for at mindske kompleksiteten ved kategorier. Eksempelvis inddeler vi millioner af farvenuancer ind i meget få farvekategorier for at mindske kompleksiteten omkring at forstå farver (J. P. Spradley, 1979). Dette betyder også, at disse kategorier kan variere en hel del i størrelse.
For at identificere kulturelle domæner, kan det derfor være essentielt at undersøge sproget der bruges af respondenterne.

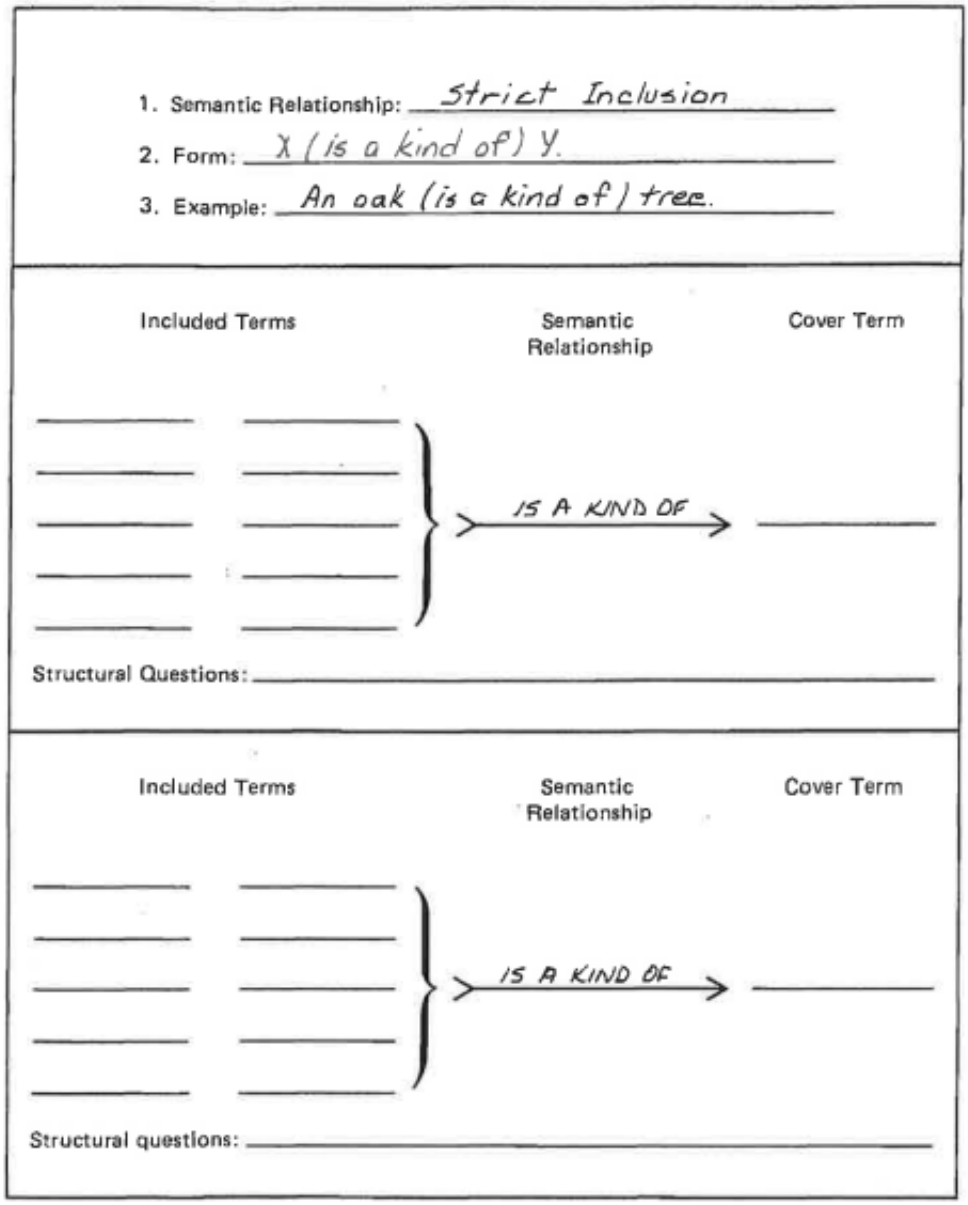
Et domæne består af et 'cover term'. Dette 'cover term' er navnet på den kategori af kulturel viden, der identificeres som et domæne. Dette kan eksempelvis være 'træ', der er 'cover term' for kulturel viden omkring træer, såsom sorter, udseende, lokation, og lignende.
Herudover indeholder et domæne flere 'included terms'. Disse 'included terms' er sproglige termer, der hører til den kategori, der er navngivet af 'cover term'et' (J. P. Spradley, 1979). Dette vil eksempelvis være sorter af træer, hvis 'cover term'et' er træ, eller sproglige udtryk, der beskriver eller omhandler et træ. De er altså alle en del af kategorien.
Yderligere, indeholder et domæne en semantisk relation. En semantisk relation beskriver en relation mellem to begreber, og i denne sammenhæng beskrives relationen mellem et af de identificerede 'included terms' og det identificerede 'cover term'. Eksemplet med træer, vil så lede til en semantisk relation, der kunne være: En bøg er et slags træ.
Der findes flere bud på, hvor mange semantiske relationer, der findes og er relevante, men i denne rapport tages der udgangspunkt i de ni relationer, der beskrives af J. Spradley (1979). Disse relationer kan ses i figur 2.3.

1. Strict inclusion	X is a kind of Y
2. Spatial	X is a place in Y, X is a part of Y
3. Cause-effect	X is a result of Y, X is a cause of Y
4. Rationale	X is a reason for doing Y
5. Location for action	X is a place for doing Y
6. Function	X is used for Y
7. Means-end	X is a way to do Y
8. Sequence	X is a step (stage) in Y
9. Attribution	X is an attribute (characteristic) of Y

Figur 2.3: J. Spradley (1979) semantiske relationer

Endeligt har et domæne også en afgrænsning, der sætter grænsen for domænet. Dette kan dog udelukkende blive afgjort af respondenter (J. P. Spradley, 1979).

Domæneanalysen vil udarbejdes ud fra worksheets beskrevet af J. P. Spradley (1979). Et eksempel på dette worksheet kan ses i figur 2.4.



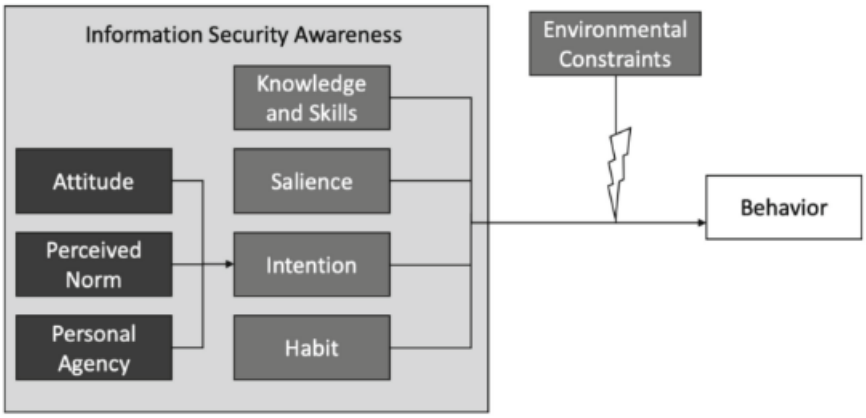
Figur 2.4: Eksempel på worksheet

Herefter samles de identificerede domæner i en liste for at skabe overblik over den kulturelle forståelse af den undersøgte organisation.

2.3.2 CSA Modenhed som kontekst for forståelsesrammerne

En af de måder organisationer kan følge deres medarbejderes cybersecurity awareness på, er ved at anvende en analyse af den organisatoriske modenhed som organisatorisk opmærksomhed. En modenhedsmodel, der ofte anvendes i CSA kontekst er Integrated Behavioral Model (IBM), som anvendes til at forklare, hvilke aspekter der påvirker menneskelig adfærd (Fertig m.fl., 2020). En af udfordringerne ved CSA er, at det kan være svært at udforme brugbare metrikker som kan vise

en udvikling i organisationen. Det ses ofte i organisationer, at et budget for CSA skal godkendes, men det kan være udfordrende at retfærdiggøre, hvis man ikke kan bevise en fremgang. Hertil kan modenhedsmodeller være gavnlige, da de beskriver metrikker som kan anvendes og måles på, men samtidig kan undersøge, hvilke områder, der er relevante at arbejde på. Grundlaget for at anvende en modenhedsmodel, der bruger metrikker som beskriver medarbejderes psykologi, er som tidligere beskrevet fordi at mennesket er en af de mest centrale elementer i cybersikkerhed hos organisationer.



Figur 2.5: Fertig m.fl. (2020) cybersecurity awareness modenhedsmodel

Fertig m.fl. (2020) kommer i deres undersøgelse frem til at medarbejdere anvender deres teoretiske viden om CSA i en af de tre følgende perspektiver:

- Medarbejdere ved at sikkerhedsbrister findes, og kan genkende dem. Dette kaldes i teorien for *perception*.
- Medarbejdere ved yderligere hvordan de kan beskytte sig selv imod sikkerhedsbrister. Dette kaldes i teorien for *protection*.
- Medarbejdere ved hvad en sikkerhedsbrist er, hvad de skal gøre, og de udfører den korrekte handleplan. Dette kaldes i teorien for *behavior*.

Dette kommer de frem til på baggrund af IBM modenhedsmodellen, der siger at en medarbejders awareness niveau er en kombination af deres overbevisninger, deres viden og evner.

En af betingelserne for at en organisation kan højne deres CSA niveau er at medarbejderne er compliant med organisationens vedtagne politikker. Ligeså skal organisationen også sikre sig at medarbejderne har de korrekte værktøjer og handlekraft til at være compliant. For at en effektiv CSA tilgang i organisationen skal fungere, er det vigtigt at der ikke er barrierer i vejen for at medarbejderne kan handle i overensstemmelse med politikkerne. I teorien bliver der anvendt et eksempel hvor medarbejdere skal skifte deres passwords regelmæssigt, men for at kunne gøre dette skal de manøvre dybt i organisationens intranet, hvor informationen er udfordrende at tilgå. Derfor er der sammenhængen mellem systemernes brugbarhed og organisationens CSA også en relevant faktor.

3 | Analyse

Det følgende afsnit vil indeholde en analyse af de foretagede interviews med medarbejdere i Hjørring Kommune. Formålet med denne analyse, er at undersøge rapportens forskningsspørgsmål, der kan ses i afsnit 1.3.
Analysen begynder med en kortlægning af de teknologiske forståelsesrammer hos medarbejdere i organisationen. Som beskrevet tidligere, vil denne analyse være den bærende del af undersøgelsen, hvor målet er at undersøge, hvordan medarbejderes fortolkninger og forståelser for begrebet CSA har betydning for arbejdet med at forankre CSA i organisationen.
Efterfølgende vil konteksten for disse forståelsesrammer analyseres. Dette gøres for at undersøge hvorvidt denne kontekst og de organisatoriske opmærksomheder har indflydelse på forståelserne og fortolkningerne af CSA.
Undersøgelsen af konteksten vil som beskrevet i afsnit 2.3, ske ved en analyse af den kulturelle kontekst og den generelle kendskab til begrebet ved at undersøge organisationens modenhed. Dette gøres for at undersøge, hvorvidt disse organisatoriske opmærksomheder har indflydelse på de teknologiske forståelsesrammer, der kortlægges. Til sidst vil følge en opsamling af hele analysen.

3.1 Kortlægning af teknologiske forståelsesrammer omkring CSA

Dette afsnit af analysen vil, som tidligere beskrevet, undersøge forståelserne af CSA hos medarbejdere i Hjørring Kommune og hvorvidt disse forståelser kan have betydning for forankringen af CSA på et organisatorisk niveau på tværs af hele organisationen. Analysen tager, som beskrevet i afsnit 1.2, udgangspunkt i Orlikowski og Gash (1994) teori om teknologiske forståelsesrammer, men det er igen værd at bemærke, at disse tager udgangspunkt i et specifikt IT-system og forståelsen omkring dette specifikke system. I denne rapport anvender vi Orlikowski og Gash (1994) teori omkring teknologiske forståelsesrammer omkring begrebet cybersecurity awareness og ikke et specifikt system. Vi mener, at teknologiske forståelsesrammer er relevante i denne sammenhæng, da CSA er et forholdsvist nyt begreb, der kræves en fælles forståelse omkring for at arbejde med, lig et IT-system. Yderligere vil det at belyse forståelser og identificere eventuel inkongruens mellem forståelsesrammer, give anledning til at arbejde med denne og skabe en uniform forståelse af CSA i organisationen. Det kan tænkes, at en sådan fælles forståelsesramme vil have positiv indflydelse på arbejdet med at forankre CSA i en organisation.

Respondenterne i undersøgelsen spænder bredt på tværs af samarbejdsorganisationen - lige fra skolelærer til bibliotekar til leder af databeskyttelses-teamet. Empirien er, som tidligere beskrevet, indsamlet gennem kvalitative interviews med disse respondenter. Empirien blev efterfølgende behandlet ved en induktiv tilgang, hvor uddrag fra interviews blev udvalgt i forhold til om de sagde noget om respondentens forståelse af cybersecurity awareness - dette indebar viden omkring begrebet, forståelse, antagelser, forventninger og lignende (Orlikowski & Gash, 1994)

Herefter lagde disse uddrag fundament for overordnede temaer og kategorier, der blev videreanalyseret og kodet, så der til sidst blev dannet områder, der dækkede over empirien. Orlikowski og Gash (1994) beskriver disse områder som domæner, men domæne-termet allerede bliver brugt i domæneanalysen, vil det blive refereret til som områder, for at skabe klarhed. Disse identificerede

områder, er derfor opstået ud fra empirien og følger derfor den induktive tilgang i dette projekt. De tre områder, der blev identificeret, kaldte vi *Hvad er CSA?*, *Hvorfor CSA?* og *Hvordan kommer CSA til syne?*.
Hvad er CSA drejer sig om forståelsen og fortolkningen omkring begrebet og dertilhørende teknologier.
Hvorfor CSA omhandler forståelsen for, hvorfor CSA er vigtigt, hvorvidt det overhovedet er vigtigt og hvilken værdi det kan skabe.
Hvordan kommer CSA til syne drejer sig om forståelsen for, hvordan begrebet kommer til syne i hverdagen, og hvilke fordele eller konsekvenser dette har i hverdagen.

Den følgende analyse vil undersøge de teknologiske forståelsesrammer omkring CSA ud fra disse områder.

Medarbejdere, der arbejder med databeskyttelse	**Medarbejdere i andre kommunale stillinger**
Medarbejder i databeskyttelsesteam	Skolelærer
Medarbejder i databeskyttelsesteam	Bibliotekar
Afdelingsleder, Sekretariatet	Demenskonsulent
	Afdelingsleder, Handicapområdet

Tabel 3.1: De identificerede grupper i empirien - egen tilvirkning

Som det kan ses i ovenstående tabel, er respondenterne delt op i to grupper - medarbejdere der arbejder med databeskyttelse til dagligt, og medarbejdere i andre kommunale stillinger. I den indledende analyse af områder, har det vist sig, at en analyse af disse to grupper vil være fordelagtig i forhold til forståelsesrammer af CSA. I den følgende analyse, vil forståelsesrammer for medarbejdere, der arbejder med databeskyttelse først blive analyseret. Efterfølgende vil medarbejdere i andre kommunale stillingers forståelsesrammer analyseres og til sidst vil en sammenligning af disse rammer følge, for at undersøge om der kan, eller bør, arbejdes med forståelsen af CSA i Hjørring Kommune. Disse forståelsesrammer vil analyseres ud fra de områder, som blev udledt ud fra de kodede uddrag.

3.1.1 Teknologiske forståelsesrammer for medarbejdere i databeskyttelse

Dette afsnit indeholder en undersøgelse af forståelsesrammerne for medarbejdere, der arbejder med databeskyttelse i Hjørring Kommune. Som beskrevet tidligere, består denne gruppe af to medarbejdere, der arbejder med databeskyttelse i form af at håndtere opståede hændelser, men også ved at optimere og forbedre processer omkring databeskyttelse, og en afdelingsleder i sekretariatet. CSA er en del af dette arbejde.

Hvad er CSA?

I og med, at medarbejderne i denne gruppe arbejder med databeskyttelse i forskellige former til dagligt, bliver det klart fra begyndelsen af interviewene, at forståelsen af CSA er på et bredt niveau. Der tænkes i CSA på tværs af organisationen som et strategisk værktøj, og ikke som et begreb for en IT-afdeling.

> *"For mig, så er det opmærksomheden omkring databeskyttelse i bred forstand. Det er alle aspekter af det. På alle platforme og på alle måder ... For mig handler det om at se på databeskyttelsen fra medarbejdernes synspunkt. Og hvordan kan jeg hjælpe dem til at gøre deres arbejde. Databeskyttelsesmæssigt mest compliant"*
> (Medarbejder, Databeskyttelsesteam - Bilag 5, 24:43, [5.10])

En lignende forståelse findes hos kollegerne i databeskyttelsesteam'et. Her beskrives en forståelse af, at CSA er "dét, at være opmærksom på cybersecurity, lade det være en fast del af hverdagen i organisationen og holde sig opdateret hele tiden"(Se bilag A.6).

Respondenterne i denne gruppe viser altså en forståelse af CSA, der ikke kun gælder deres egen hverdag. De udviser ligeledes et forsøg på at forstå alle andre medarbejdere i organisationens forståelse af CSA.
Dette nævnes også af medarbejdere i denne gruppe, der i denne sammenhæng forstår, at CSA er "et besværligt emne, da det er fluffy og svært at få medarbejdere til at forholde sig til, da der ikke er et decideret facit"(Se bilag A.7).
Denne forståelse af, at CSA er en konstant udvikling eller ikke har et decideret facit eller slutresultat, går altså igen for denne gruppe af respondenter.

En anden forståelse, der går igen i denne gruppe, er en forståelse af et ansvar omkring CSA i organisationen. Dette ansvar stammer i høj grad fra, at det er deres arbejde, men udviklingen bevæger sig dog i en retning, hvor ansvaret i lige så høj grad lægges hos den enkelte medarbejder i alle stillinger i organisationen. Det vil sige, at medarbejdere i denne gruppe i lige så høj grad arbejder med forandringsledelse i form af at få medarbejdere i andre stillinger til at tage dette ansvar til sig.
Dette kommer også til syne i deres forståelse af CSA, da de mener, at dette skal "indlejres i kulturen i organisationen og hos de enkelte individer ved at sætte fokus på cybersecurity awareness. Det er ikke blot en opgave for IT-afdelingen, men det er dog dem, der skal være bedre til at få alle med på det"(Bilag 6).
Der er altså en forståelse af ansvar for CSA i denne gruppe, men også en forståelse af, at dette ansvar bør bredes ud i organisationen. Forståelsen af ansvaret i denne gruppe i forhold til CSA, bliver derfor i stedet et ansvar for at få udbredt ansvaret af CSA i organisationen.

Yderligere viser denne gruppe en forståelse af, at CSA er en kontinuerlig proces, der ikke kan sættes et facit under (Bilag 7). Derfor er de alle enige om, at det kræver en bred forståelse i organisationen omkring CSA og værdien, det skaber.
Deraf kommer forståelsen af ansvaret omkring at få udbredt det i organisationen.

Hvorfor CSA?

Dette område omhandler gruppens forståelse af, hvorvidt CSA er vigtigt og i den forbindelse, hvorfor det er vigtigt.
Respondenterne i denne gruppe har en forståelse af, at CSA er essentielt, fordi der behandles personfølsomme og private data i hele organisationen. Data er en del af den daglige hverdag, så der er en forståelse for, at det er nødvendigt at behandle denne data.

> *"Og det er jo i alt, hvad de laver. Det er jo de iPads, hjemmeplejen har med rundt. Det er de røntgen billeder, tandplejen tager af skolebørnene. Det er i det hele. Men det er jo også, når borgeren melder ind, at lyset er gået på deres villa-vej. Og nu faldt deres mor og brækkede hoften og er nu indlagt. Så får vi på den måde en masse personhenførbare oplysninger, som jo også kan være følsomme eller fortrolige"*
> (Medarbejder, Databeskyttelsesteam - Bilag 5, 03:40, [5.11])

Samtidig er der også en forståelse af, at CSA er vigtigt netop fordi data er i alting, og det derfor automatisk bliver en del af alle medarbejderes kerneopgaver at behandle denne data korrekt. Dette gælder både medarbejdere i IT-afdelingen, men også alle andre i organisationen.

> *"Så det der med at få det tydeliggjort, hvorfor det er vigtigt at huske og agere databeskyttelsesmæssigt korrekt for at kunne udføre sin kerneopgave"*
> (Medarbejder, Databeskyttelsesteam - Bilag 5, 04:26, [5.12])

Der er derfor en forståelse for, at CSA kræves fordi data bliver så udbredt, at det ikke længere er muligt for en IT-afdeling at stå med ansvaret alene. Dette kan ligeledes være grunden til, at begrebet CSA blev til.
Denne udbredelse af CSA er dog voksende, til dels på baggrund af, at der også kommer større fokus på det i det private liv. Dette øgede fokus vil derfor lede til en større bevidsthed omkring CSA i organisationer, ifølge respondenterne i denne gruppe (Se bilag A.6).

Hvordan kommer CSA til syne?

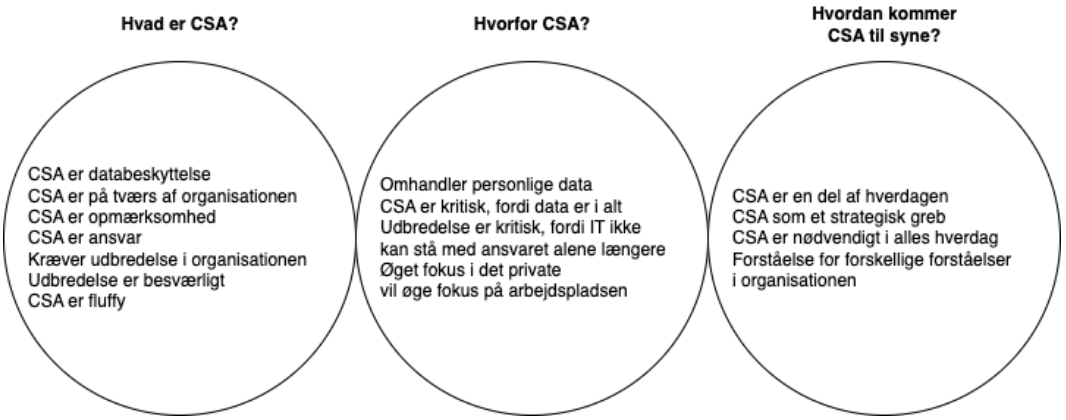
CSA kommer til syne i denne gruppes hverdag i form af deres daglige arbejdsopgaver. Respondenterne i denne gruppe arbejder med databeskyttelse til dagligt og CSA er derfor en naturlig del af deres arbejdsopgaver. Der er en forståelse for, at det er nødvendigt, at CSA også kommer til syne hos medarbejdere uden for databeskyttelsesteamet, hvilket også ses i de foregående områder. Dette betyder, at CSA i høj grad kommer til syne på et strategisk niveau.
Dette strategiske niveau kommer til syne i en forståelse af, at der findes forskellige forståelser af CSA, som der skal tages højde for i forsøget på at udbrede denne forståelse (Se bilag A.6). Dette går ligeledes tilbage til forståelsen om, at mange medarbejdere tror, det ikke er en del af deres kerneopgaver.
Der er altså en interessant observation her omkring, at respondenter i denne gruppe er klar over, at der findes forskellige forståelser af CSA på tværs af organisationen. Dette betyder, at CSA, i denne gruppe, kommer til syne ved at de arbejder med disse forskellige forståelser, i deres forsøg på at udbrede CSA.

Forståelsesramme for medarbejdere i Databeskyttelsesteam

De foregående afsnit har undersøgt forståelsesrammen omkring CSA for medarbejdere, der arbejder med databeskyttelse ud fra de tre identificerede områder.
Medarbejdere i denne gruppe har en forståelse af, at CSA er nødvendigt og kritisk i en moderne organisation, hvor data indgår i alting. Dette betyder, at det er nødvendigt at behandle denne data rigtigt.
Dette medfører et ændret syn på, hvor ansvaret for arbejdet med CSA ligger. Da håndteringen af

data snart sker i alle stillinger, forstår denne gruppe, at det er nødvendigt, at alle har et ansvar for at håndtere denne data sikkert og korrekt. Ansvaret skal derfor bredes ud i organisationen, hvad angår CSA. Dog har denne gruppe en forståelse af, at de har ansvaret for, at denne udbredelse sker, da de arbejder med det til dagligt.

Forståelsen for CSA i denne gruppe befinder sig derfor på et strategisk niveau, hvor der tænkes i forbedringer og optimeringer af databeskyttelsen. CSA fungerer som et værktøj for at øge effektiviteten af databeskyttelsen i kommunen.
I den forbindelse er CSA en essentiel del af denne strategiske tænkning, da det ikke længere er muligt for en IT-afdeling alene at stå for IT-sikkerheden. CSA kommer derfor oftest til syne for denne gruppe i form af forsøg på at udbrede begrebet i hele organisationen. Dette betyder, at det ofte er i form af forandringsledelse og oplysning/oplæring, at CSA kommer til syne i hverdagen. Forståelsesrammen for denne gruppe kan ses i nedenstående figur 3.1.



Figur 3.1: Visualisering af forståelsesramme for medarbejdere, der arbejder med databeskyttelse - egen tilvirkning

3.1.2 Teknologiske forståelsesrammer for medarbejdere i andre kommunale stillinger

Dette afsnit undersøger forståelsesrammer for medarbejdere i andre kommunale stillinger i Hjørring Kommune. Denne gruppe består af fire medarbejdere i vidt forskellige stillinger, som tidligere beskrevet i analysen. Analysen af denne gruppe vil foregå på samme vis som analysen af den forrige gruppe, ud fra de tre identificerede områder.

Hvad er CSA?

Denne gruppe indeholder medarbejdere i Hjørring Kommune fra vidt forskellige stillinger i organisationen. Det bliver derfor hurtigt klart, at forståelsen for, og opfattelsen af, cybersecurity awareness udspringer fra den hverdag som den enkelte befinder sig i. I starten af hvert interview bad vi respondenten om at skrive tre ting ned, som vedkommende umiddelbart tænker på når vi sagde ordene 'cybersecurity'. Vi gjorde dette både for at spore deres tanker ind på det overordnede term, for efterfølgende at undersøge deres forståelse af CSA. Her blev de bedt om at fysisk skrive noget ned på et stykke papir (dette var ikke muligt ved interviews over Teams, hvorfor de i stedet skrev

i chatten i stedet), men også for at få et indblik i deres nuværende overordnede forståelse af cybersecurity og CSA. Dette blev gjort inden vi havde snakket omkring begrebet og må derfor anses som værende deres umiddelbare tanker og forståelse omkring CSA. Denne øvelse ledte til flere forskellige forståelser.

> *"Cybersecurity for mig er i hvert fald noget med at forebygge og være sikker på, at man er på forkant med de ting, der kan ske i organisationen, som vi er i."*
> (Skolelærer i specialklasse - Bilag 1, 01:45, [1.1])

Én forståelse kommer til syne i form af forebyggelse. Her ses cybersecurity awareness som dét at kende til de trusler, der kan true organisationen, være på forkant med disse og på den måde forebygge. En lignende forståelse lyder således:

> *"Altså, at man er særlig obs på det som udviklingen det byder på. Jeg tænker på, det handler om at udviklingen, den rykker sig hele tiden, så vi skal være sikre på, at når vi introducerer nye systemer eller nye teknikker, eller der kommer et nyt medie, noget vi ikke kan forudsige konsekvenserne af, der skal man være særlig opmærksom på, at.."*
> (Afdelingsleder, Handicapområdet - Bilag 2, 07:13, [2.5])

Her ses igen en forståelse af CSA som værende en udvikling, der skal tages højde for og som man skal være bevidst om kan skabe muligheder, men ligeledes trusler for en organisation.

En anden forståelse af CSA, der kommer til syne i denne initierende ord-øvelse, er baseret mere i den daglige hverdag for respondenterne. Dette ses blandt andet ved, at en bibliotekar skriver keylogging som et ord, da biblioteker har været udsat for en del keylogging angreb. Denne indflydelse som den enkeltes hverdag har på forståelsen af CSA kommer ligeledes til syne i følgende citat:

> *"Nu har jeg været en del af det her med at lave en hjemmeside indenfor mit område og jeg er mest bekendt med GDPR i forhold til det her med billeder, fordi vi har Facebook, vi har hjemmesider, instagram, vi har alt muligt som profilerer os og fortæller om, hvordan er det at være handicappet i Hjørring Kommune og,hvad laver vi rent faktisk"*
> (Afdelingsleder, Handicapområdet - Bilag 2, 02:01, [2.1])

I dette citat bliver GDPR ligeledes nævnt. Netop GDPR gik igen et par gange i disse indledende ord. Dette blev ofte nævnt i forbindelse med tidspunkter i hverdagen, hvor GDPR forhindrer eller besværliggør opgaver, som det eksempelvis ses i ovenstående citat omkring upload af billeder til hjemmesider og sociale medier. Denne forståelse af, at CSA kan være en hindring i de daglige opgaver kommer dog ikke kun til syne hos respondenterne i forhold til GDPR. Det kommer ligeledes til syne i et bredere perspektiv:

> *"...men jeg synes, det giver noget pangel. Det bliver sådan lidt tungt, nogen gange"*
> (Afdelingsleder, Handicapområdet - Bilag 2, 13:21, [2.9])

Det viser sig også i interviews med respondenterne, at det ikke er alle, der har en forståelse af cybersecurity awareness. Således er det ikke alle, der har en forståelse for, at CSA er et begreb, der findes.

> *"Det er bare det der cyber-awareness, det var jeg ikke engang klar over, at det var et begreb, tænkte jeg. Okay, hold da op"* (Demenskonsulent - Bilag 3, 09:41, [3.9])

Den generelle forståelse for CSA blandt medarbejdere med traditionelle kommunale stillinger, omhandler altså i høj grad deres stilling og hverdag. Som det kan ses i nogle af citaterne, er der ligeledes en forståelse for, at cyber trusler er noget, der skal forebygges ved at være bevidst om udviklingen af teknologi og forhindre cyberhændelser ved forebyggelse. Denne forebyggelse ses mest som logivning eller praksisser i organisationen i forhold til deres forståelse - eksempelvis i form af GDPR, der således kommer til syne i deres hverdag. Denne forståelse viser sig også som en proces eller en opgave, der er uendelig i den form, at udviklingen gør, at man skal være opmærksom og selv udvikle sig i takt med denne udvikling.

> *"Jamen jeg tror, jeg mener faktisk lidt det som jeg, det man kan sige med processen, at man ikke er færdig, man kan ligesom godt tænke at vi er dækket af, at vi sådan har brandsikret eller prøvet sådan at fremtidssikre os lidt mod et eller andet, men der er jo bare, der sidder bare nogle kloge mennesker et eller andet sted med nogle rimelig trælse hensigter også, som nok skal komme videre end det. Så derfor skal vi også bevæge os hele tiden, altså og så kan man sige, hvad er det? Og det ved vi måske ikke fordi den ikke er bygget endnu. Giver det mening?"*
> (Bibliotekar - Bilag 4, 04:30, [4.4])

Hvorfor CSA?

Uddragene fra interviewene viste i høj grad, at grunden til eller formålet med CSA, er en vigtig del af både forståelsen for, hvorfor der er fokus på det, men også som motivation for denne gruppe. Denne gruppe med medarbejdere i andre kommunale stillinger, efterlyser især fokus på netop formålet med CSA, da det ikke er en del af deres hovedopgaver i hverdagen, og derfor tager fokus og tid fra disse hovedopgaver.

> *"Jeg tror i høj grad, det er det. At man ikke lige helt ved, hvad det er. Er det noget teknisk, eller er det ikke noget teknisk? Har jeg egentlig forståelse, eller har jeg viden omkring det? Nej, det har jeg måske nok ikke. Så bliver det nedprioriteret på en eller anden måde. I forhold til de andre ting, der foregår i løbet af sådan en hverdag"*
> (Skolelærer - Bilag 1, 03:04, [1.4])

> *"Så jeg synes, det er vigtigt, men det bliver også lidt tungt. Så for mig er det både det ene og det andet"*
> (Afdelingsleder, Handicapområdet - Bilag 2, 02:01, [2.2])

Det er dog interessant at se på, hvordan denne forståelse af, at CSA er vigtigt opstår blandt respondenterne, da flere respondenter i stedet nævner ydre omstændigheder i omverdenen som motivator for at have fokus på CSA.

> *"Ja, det tror jeg faktisk, det bliver sådan lidt... At så hører man måske nogle historier om, at det er gået galt for nogen, fordi de har fået klikket på et eller andet forkert link eller sådan noget, ikke? Og så tænker man, at det skal man nok lige lade være med"*
> (Demenskonsulent, Bilag 3, 09:41, [3.9])

Dette er et eksempel på, at det bliver omverdenen, der har indflydelse i, hvorfor respondenter forstår vigtigheden af CSA. Det kommer ligeledes til syne i følgende citater:

> *"...men måske også en, det ved jeg ikke, verden er jo et rodet sted pt, at ting er mere sårbare måske, end man sådan lige regner med, og man skal jo ikke bladre i ret mange aviser før man ser nu er det her nede, den her er blevet hacket og sådan noget i den stil. At noget man sådan har tænkt der er meget robust før, det er måske der den ligger i awareness tingen, at der er sådan en instabilitet, skrøbelighed indbygget sådan samfundsmæssigt også lige pludseligt, at man ikke skal regne med noget og SAS går ned eller et eller andet i den stil. Altså der er ikke noget som er sikkert, sådan længere på en eller anden måde. Så derfor får man også lyst til måske at sikre sig så godt som man kan ikke, og ja, giver det mening"*
> (Bibliotekar - Bilag 4, 12.00, [4.9])

> *"Fuldstændig, men noget som også gøder det er jo for eksempel sådan noget som nyheder, når man så ser at alt muligt bare bliver hacket fra en side af, eller at der har været brud på et eller andet, det ville jeg så også våge at påstå at er med til det implicit. At folk kommer i tanker om, som jeg også nævnte før at verden er bare mere usikker end man måske tror"*
> (Bibliotekar - Bilag 4, 24:41, [4.20])

Det kommer til syne i disse citater, at det i høj grad er skrækhistorier fra omverdenen, der sætter fokus på vigtigheden ved CSA. Dette er en interessant observation, da det i høj grad indikerer, at der i en bredere grad er fokus på netop CSA. Der er dog også en interessant modsigelse i netop dette, hvis man ser på denne gruppes forståelse af CSA, som blev belyst før. Her blev forståelsen beskrevet som at følge med i udviklingen og på den måde forebygge disse trusler. Denne forebyggende forståelse er dog lidt modsat af forståelsen af, hvorfor CSA er vigtigt, da denne bygger på skrækhistorier fra omverdenen. Det bliver altså en reaktion mod historier fra andre, og ikke en forebyggende forståelse, som beskrevet tidligere.

En anden interessant forståelse, der kommer til syne i de afholdte interviews, er respondenternes syn på deres egen forståelse af CSA modsat deres kollegers. Her kom det ofte til syne, at der er en forståelse af, at den enkelte forstår deres egen forståelse af CSA som værende større eller anderledes end deres kolleger - eller i hvert fald forståelsen af vigtigheden af CSA. Dette kan blandt andet ses i nedenstående citat.

> *"Når jeg hører det, så tænker jeg jo, at det er det her med at være bevidst om, at det er noget, der er vigtigt. Det tror jeg faktisk ikke, at der er mange, der er. Dem, som måske har en lille smule IT-snilde, de ved nok godt, hvad det handler om. I min organisation, der vil jeg tro, at 80% af vores stab, vil nok ikke helt vide, hvad det handler om"*
> (Skolelærer - Bilag 1, 03:04, [1.4])

Denne forskellige forståelse af vigtigheden kommer ligeledes til syne andre steder i kommunen, blandt andet på biblioteket:

> *"Så kan man sige, det er spændet på awareness-delen, den viser det faktisk meget godt, at der er nogen, jeg er sådan lidt fascistoid omkring det og låser også andres computere, hvis jeg lige kommer forbi en, så siger jeg lige plup og så, men der er også andre som tænker, årh det går nok, jeg skal bare lige herover"*
> (Bibliotekar - Bilag 4, 17:33, [4.13])

Disse citater viser en interessant deling i forståelsen af, hvorfor CSA er vigtigt. Det er tydeligt, at alle respondenter har en fælles forståelse af, at CSA og sikkerhed generelt er vigtigt, hvad end denne forståelse er skabt af skrækhistorier fra omverdenen eller internt i organisationen. Der viser sig dog også en forståelse - eller måske misforståelse - af kollegernes forståelse. Det virker altså til, at respondenterne har en forståelse af, at deres egen forståelse af vigtigheden af CSA er anderledes end deres kolleger. Dog er dette synligt hos alle respondenterne, vi snakkede med. Dette kommer også til syne i deres forståelse af, hvordan og hvor meget CSA fylder - og skal fylde - i deres hverdag. Dette vil blive undersøgt i det kommende afsnit.

Hvordan kommer CSA til syne?

Dette domæne omhandler denne gruppes forståelse af, hvordan CSA kommer til syne i deres hverdag. Den indsamlede empiri viser, at CSA kommer til syne for denne gruppe på forskellige måder, da det i høj grad afhænger af deres stilling i kommunen og deres daglige opgaver. Eksempelvis, som vist tidligere, kommer CSA blandt andet til syne på biblioteker i form af borgernes brug af åbne netværk på biblioteket. Anderledes er det for skolelærere, hvor CSA kommer til syne i deres arbejde med børnene og deres personlige informationer. Igen anderledes er det for en afdelingsleder på handicapområdet, der oplever CSA i hverdagen i forhold til rettigheder til anvendelse af billeder af medarbejdere og medlemmer.

Som empirien har vist tidligere, fører denne forskellighed i hverdage også til forskellige forståelser af CSA, da det bliver klart, ud fra respondenternes udsagn, at forståelsen af CSA i høj grad formes ud fra den hverdag man befinder sig i.

Flere af de interviewede respondenter, gav i denne sammenhæng udtryk for, at CSA og den generelle sikkerhed af interne systemer, er noget, der bliver klaret i IT-afdelingen. På den måde kommer det ikke til syne hele tiden i deres hverdag.

> *"Jeg tror, der er mange, der tænker, at vores IT-mand, han styrer det der"*
> (Skolelærer - Bilag 1, 07:36, [1.8])

> *"Ja, man kan sige beskyttelsen udadtil, den er todelt hos os, fordi vi har jo ligesom, vi har en IT infrastruktur hos os, men den er ude i en armslængdeprincip fordi at vores infrastruktur, altså i huset, den bliver lavet hernede et eller andet sted, vi bor jo et andet sted, så det er lidt distanceret på en eller anden måde, det er ikke sådan noget vi, det er meget kommunalt ikke, det er noget IT de tager sig af, det fikser de nok, det er sådan den ene del af det. Men så har vi så vores, hvad hedder det, vores fagsystem, vores biblioteksystem, vores hjemmesidedrift og det er ligesom, det kører et andet sted fra, så det er sådan, jeg tror måske nok det måske er en lidt usund tankemæssigt at det er distanceret og ikke er noget vi selv har styr på, men samtidigt med så ved jeg at dem som sidder i den anden ende og tager sig af det, de har markant mere styr på det, altså vi har ikke ressourcer til at have IT personale der kan styre sådan noget, men det gør måske også lidt at sådan tankesætsmæssigt, så er det ikke så present i hverdagen, der er styr på det regner vi med"*
> (Bibliotekar - Bilag 4, 09:07, [4.7])

Det viser sig altså, at der i hverdagen er en bred forståelse for, at IT-afdelingen klarer de sikkerhedsmæssige aspekter af det IT-mæssige i organisationen. Dog er det også værd at bemærke, at blandt andet bibliotekaren nævner, at det kan blive en udfordring at have denne tankegang, da det i så fald fjerner fokus fra CSA i deres hverdag. På den måde udvises der også en højere forståelse for, at der er behov for mere CSA i hverdagen. Denne forståelse deles dog ikke af alle. Flere respondenter giver udtryk for, at de ikke mener, CSA skal fylde mere i deres hverdag.

> *"Det fylder jo ikke meget. Det er nok mere i min underbevidsthed, tror jeg. Jeg tror ikke, jeg synes, det skal fylde mere for mig. Men jeg tror måske, at jeg synes, det skal fylde mere på bredt plan. At der er flere, der er klar over det, og flere, der er med på, hvordan vi gør for at forhindre de ting"*
> (Skolelærer - Bilag 1, 07:01, [1.7])

> *"Nej, det fylder ikke så meget (CSA, red.). Det fylder i perioder, som for eksempel når jeg har sat hjemmesiden op og sådan, så fylder det i en lang periode. Så skal der sorteres i nogle billeder og så skal man tænke på det med samtykke. Når det så er færdigt, så kører der en procedure for det. Men det kan godt være, vi mangler sådan nogle awareness programmer som man lige kunne køre igennem. På vores onboarding plan for eksempel"*
> (Afdelingsleder, Handicapområdet - Bilag 2, 14:49, [2.11])

Denne forståelse af, at CSA ikke skal fylde mere kan ses i forbindelse med, hvornår i hverdagen respondenterne oplever, at CSA kommer til syne. Da vi adspurgte respondenterne om dette, svarede de, at det oftest var når CSA var bøvlet i forhold til deres arbejdsopgaver, og dermed bliver en hæmsko.

> *"Det er mest der, hvor jeg opdager, at jeg ikke har tænkt mig om. Altså cookies, og så opdager jeg pludselig, at nu føler jeg mig lidt indskrænket fordi, at jeg har sagt ja til cookies på lige præcis det her område. Det er mere det. Så bliver jeg lidt forskrækket over, kunne du måske have sat dig lidt mere ind i det"*
> Afdelingsleder, Handicapområdet - Bilag 2, 09:25, [2.18])

> *"Så bliver det nedprioriteret på en eller anden måde. I forhold til de andre ting, der foregår i løbet af sådan en hverdag"*
> (Skolelærer - Bilag 1, 06:21, [1.6])

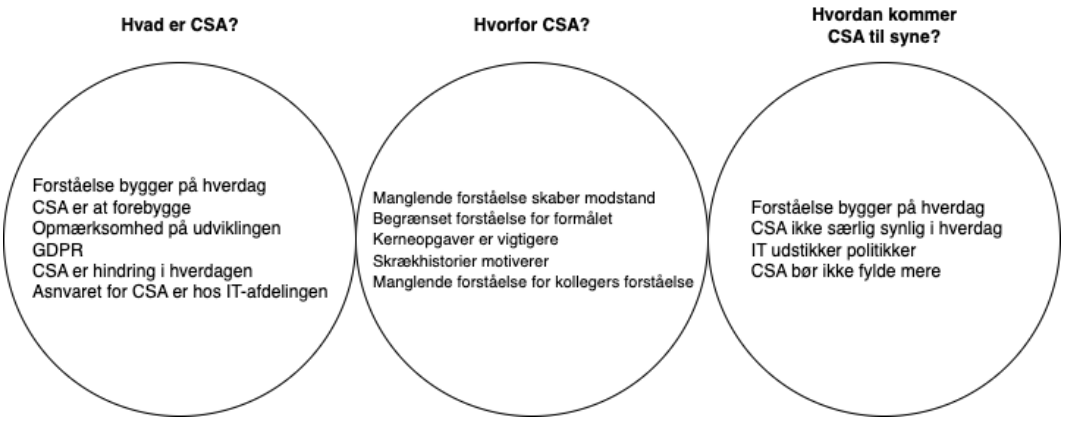
> *"...og der vælter jo frem med ting og sager fordi man, fordi der er hverdag og man kan godt gå og tænke, det skal vi også lade være med at gøre og vi skal gøre sådan her. Men det skal også være færdig klokken et i dag, så jeg skynder mig lige og lave et eller andet"*
> (Bibliotekar - Bilag 4, 05:05, [4.5])

Dette syn på CSA som en hindring i hverdagen medfører altså, at det bliver nedprioriteret. Det ses ligeledes, at medarbejdere retfærdiggør denne nedprioritering, som Barlow m.fl. (2013) teoriserer, i deres teori omkring, hvorfor medarbejdere bryder politikker omkring sikkerhed.
Dette medfører en forståelse af CSA som værende mindre vigtigt end kerneopgaverne i hverdagen for denne gruppe.

Forståelsesramme for medarbejdere i andre kommunale stillinger

Medarbejdere i andre kommunale stillinger har en forståelse af, at CSA handler om at være opmærksom på udviklingen af teknologi og på den måde forebygge angreb. Alle respondenter i denne gruppe forstår, at CSA er vigtigt, men der er tilgengæld forskel på, hvorfra denne forståelse opstår. For de fleste opstår den i omverdenen, eksempelvis via skrækhistorier fra andre organisationer. Der er dog alligevel også en fælles oprindelse af denne forståelse i form af lovgivning eller praksis, der bliver indført højere oppe fra, eller fra en IT-afdeling. Dette kan eksempelvis være i form af GDPR eller andre politikker, der indføres. Dette bliver styrket af en forståelse af, at der er andre - IT-afdelingen - som har styr på det med cybersecurity.
I denne forståelse ligger også, at det er en IT-afdeling, der har ansvar for CSA. Derfor er der også en forståelse af, at CSA ikke burde fylde mere i hverdagen for respondenter i denne gruppe.

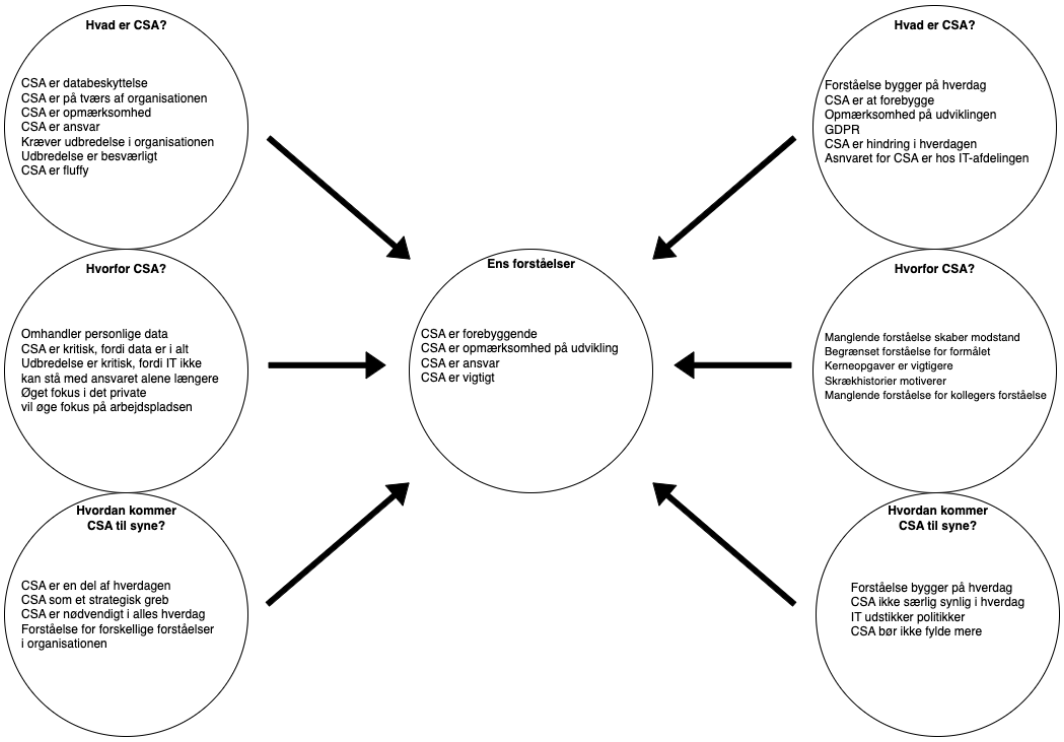
En visualisering af denne gruppes forståelsesramme i forhold til CSA kan ses i figur 3.2.



Figur 3.2: Visualisering af forståelsesramme for medarbejdere i andre kommunale stillinger - egen tilvirkning

3.1.3 Sammenligning af forståelsesrammer blandt de to grupper

Dette analyseafsnit har undersøgt de teknologiske forståelsesrammer for de to identificerede grupper af respondenter i Hjørring Kommune - henholdsvis medarbejdere, der arbejder med databeskyttelse og medarbejdere i andre kommunale stillinger. Denne analyse har ført til to forståelsesrammer baseret på disse interviews, som er forsøgt visualiseret i de foregående afsnit, se figur 3.1 og 3.2.
Dette afsnit vil sammenligne disse forståelsesrammer og undersøge, hvor de ligner hinanden og, hvor der opstår forskellige forståelser.
En visualisering af dette kan ses i nedenstående figur 3.3.

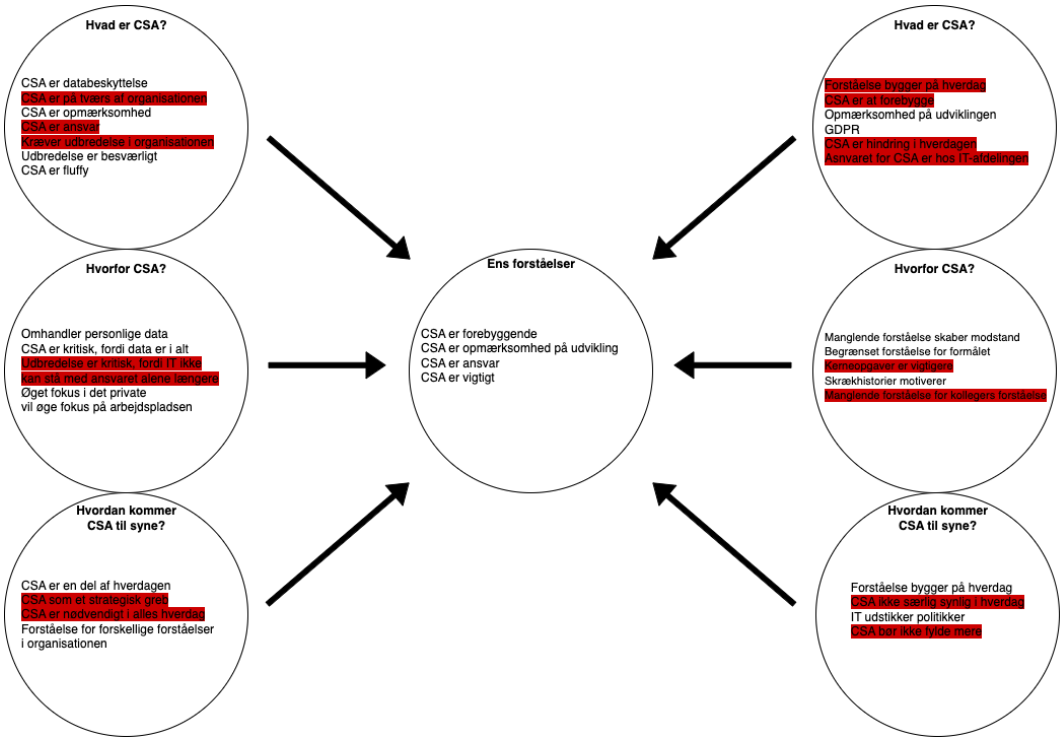


Figur 3.3: Sammenligning af forståelsesrammer - egen tilvirkning

Ser man på forståelsen af, hvad CSA er, viser analysen, at der findes både ligheder og forskelle i denne forståelse blandt de to grupper. Begge grupper forstår CSA som en udvikling. Denne udvikling kræver, at en organisation følger med, for at kunne arbejde med CSA. Der er dog en forskel i, hvordan de to grupper forstår intentionen med CSA. Gruppen med medarbejdere i andre kommunale stillinger har en fælles forståelse af, at CSA er noget forebyggende arbejde, der skal forebygge udefrakomne trusler, mens den anden gruppe både forstår CSA som værende forebyggende, men også som mitigerende under et eventuelt angreb.

Denne forskel kan ses i sammenhæng med forståelsen af ansvaret omkring CSA blandt de to grupper. Her viser analysen i hvert fald, at der findes en klar forskel i forståelsen. Gruppen med medarbejdere i andre kommunale stillinger forstår, at CSA er IT-afdelingens ansvar, mens IT- og databeskyttelsesteamet forstår, at ansvaret skal bredes ud hos alle i organisationen, da alle arbejder med IT og data. Denne forskellige forståelse af, hvor ansvaret ligger i forhold til CSA, kan åbenlyst føre til udfordringer i hverdagen. Medarbejdere i andre kommunale stillinger, forstår altså ikke CSA

som en del af deres kerneopgaver, og derfor er det IT-afdelingens ansvar. Hvis IT-afdelingen forstår det omvendt, kan det føre til udfordringer. Her opstår altså en inkongruens i forståelsesrammerne blandt de to grupper.
En visualisering af de forskellige forståelser kan ses i figur 3.4, hvor de markerede forståelser viser forskellene.



Figur 3.4: Forskelle i forståelsesrammer - egen tilvirkning

En anden interessant observation i forskellene på forståelser, er hvor meget CSA bør fylde i hverdagen.
Her mener medarbejdere i andre kommunale stillinger ikke, at CSA bør fylde mere, mens databeskyttelsestemaet prøver at udbrede CSA ud i organisationen. Dette kan ligeledes åbenlyst føre til udfordringer i organisationen. Især da der for medarbejdere i andre kommunale stillinger er en forståelse af, at CSA er en hindring i hverdagen og de daglige opgaver. Der kræves derfor en fælles forståelse for CSA blandt de to grupper - dette kunne eksempelvis være en fælles forståelse af, hvorfor CSA er vigtigt, som er det næste område, vi kiggede på.

Gruppen med medarbejdere i databeskyttelsesteamet deler en fælles forståelse af, at CSA er essentielt fordi alle stillinger i en moderne organisation behandler en eller anden form for personlig eller fortrolig data. Dette kræver så, at alle har en forståelse af, hvordan denne skal behandles og håndteres.
Denne forståelse af, at CSA er kritisk for alle, deles dog ikke af medarbejdere i andre kommunale stillinger. Her deles en forståelse af, at CSA kommer i anden række i forhold til kerneopgaverne i stillingen, der bestrides. Dette er lidt paradoksalt, da denne gruppe dog også viser en forståelse af, at CSA er vigtigt - især på baggrund af skrækhistorier fra omverdenen.

Der er også en interessant forståelse hos gruppen med medarbejdere i andre kommunale stillinger, hvor de fleste har en forståelse af, at CSA burde fylde mere for deres kolleger, men ikke i

deres egen hverdag. Det virker til, der er en inkongruens i forhold til denne forståelse, når flere respondenter fortæller det samme. Dette er dog en inkongruens blandt respondenterne i denne gruppe og ikke i forhold til medarbejdere, der arbejder med databeskyttelse. Det er dog alligevel interessant, at der indenfor in gruppe med forholdsvis ens forståelser for begrebet, ikke ved så meget om kollegernes forståelse. Om ikke andet viser det i hvert fald, at det ikke er et emne, der snakkes om eller diskuteres ofte i hverdagen.

Ser man på, hvordan CSA kommer til syne i hverdagen hos de to grupper, er forståelserne også forskellige. Medarbejdere i andre kommunale stillinger oplever ofte, at CSA kommer til syne i form af politikker, der er udstukket andre steder fra, men også når det er en hindring for deres kerneopgaver. Disse politikker udstikkes af IT-afdelingen, hvor CSA kommer til syne i alle dele af deres hverdag. Her kommer CSA dog til syne på et strategisk niveau, da der tænkes i at udbrede CSA på den bedst mulige måde.

Denne analyse har vist, at der findes inkongruens i forståelsesrammerne blandt de to grupper af respondenter i Hjørring Kommune. Dette gælder især ansvarsfordelingen i forhold til CSA, vigtigheden af CSA i forhold til kerneopgaver og hvor meget CSA bør fylde i hverdagen.
En visualisering af sammenligningen af forståelsesrammerne kan ses i figur 3.3. Disse forskelligheder i forståelse kan med fordel adresseres for at gå fra at anse CSA på et individuelt perspektiv til et organisatorisk perspektiv, da det kan være en hindring for dette. Dette leder frem til en undersøgelse af kulturen hos Hjørring Kommune angående forståelsen af CSA.

3.2 De teknologiske forståelsesrammers kontekst

Dette afsnit vil undersøge konteksten som de foregående forståelsesrammer opstår og formes i. Som Orlikowski og Gash (1994) beskriver, er disse forståelsesrammer ikke statiske, men mere flydende i deres natur, hvorfor konteksten er relevant at forstå.
Afsnittet begynder med at undersøge den kulturelle kontekst i form af en analyse af etnografiske domæner ifølge J. P. Spradley (1979).
Herefter anvendes Fertig m.fl. (2020) modenhedsmodel til at undersøge kendskabet til CSA og den organisationelle modenhed omkring CSA, for at forstå, hvordan denne organisatoriske opmærksomhed, kan påvirke forståelserne af CSA.

3.2.1 Den kulturelle kontekst

I denne del af analysen er målet at undersøge kulturen i forhold til CSA hos Hjørring Kommune. Dette gøres med empiri fra projektets interviewpersoner, som vil blive analyseret med den tidligere præsenterede teori fra (J. P. Spradley, 1979), se afsnit 2.3. Formålet med denne domæneanalyse er, at forstå kulturen omkring CSA ved hjælp af disse domæner. Som beskrevet i afsnit 2.3, lader en domæneanalyse disse domæner opstå af empirien, som empirien tillader det. Domænerne vil således være en afspejling af denne kultur, der ønskes undersøgt.
Med dette udspring i empiri, vil udtalelser og citater blive samlet under disse identificerede domæner, hvorefter de vil blive analyseret enkeltvis.

De repræsenterede domæner

De anvendte domæner i analysen blev identificeret i kodningsprocessen af empiriindsamlingen. Efter de 'included terms' blev fundet, blev der lavet en semantisk relation til det endte 'cover term'. De 'cover terms' som empiriindsamlingen gav lys til var følgende: Data, Sikker adfærd, Ændret adfærd, Ansvar, CSA forståelse, Trussel og Træning. Ens for disse domæner er, at de alle udspringer i kulturelle elementer i organisationen og tager udgangspunkt i, hvilke handlinger der er fremtrædende i interviewpersonernes hverdag, samt hvordan de forbereder sig imod de ondsindede aktører som prøver at få adgang til deres systemer.
Som tidligere nævnt er disse domæner altså opstået fra empirien, og de semantiske relationer er derfor ligeledes udarbejdet ud fra, hvor ofte de omtales i empirien.

Interviewpersonerne repræsenterer forskellige områder i virksomheden, som giver projektgruppen den bedst mulige og bredeste opfattelse af Hjørring Kommunes forståelse af begrebet, som det er beskrevet i afsnit 3.1. I dette afsnit vil respondenterne dog analyseres samlet og ikke i to grupper som det var tilfældet i tidligere analyseafsnit.

Ifølge J. P. Spradley (1979) er der ni universelle semantiske forhold til at starte en domæneanalyse, se figur 2.3.
De relevante semantiske relationer til denne domæneanalyse er; Strict Inclusion, Attribution, Rationale og Cause-effect, da den induktive undersøgelse fandt frem til ord, der samlede domæner indenfor disse semantiske relationer.
De relevante ord blev sat ind i det domæneanalyse arbejdsark som J. P. Spradley (1979) præsenterer, se figur 2.4.
Dette arbejdsark blev udfyldt i Excel. Det er vigtigt at understrege, at de inkluderede termer er de ord som interviewpersonerne brugte i forbindelse med interviewet, via den induktive tilgang. Dette var essentielt for analysen, da de fundne domæner således afspejler kulturen i Hjørring Kommune. Stjernerne ved ordene er repræsentativt for at disse ord er gentagne under andre domæner også. Nedenstående tabel 3.2 viser de identificerede domæner med dertilhørende semantiske relation.

Domæne	**Semantisk relation**	**Strukturelt spørgsmål**
Former for data	X is a kind of Y	Hvad er de forskellige slags data?
Sikker adfærd	X is an attribute of Y	Hvad er sikker adfærd?
Grund til ændret afdærd	X is a reason for doing Y	Hvad fører til ændret adfærd?
Ansvar for CSA	X is a result of Y	Hvad fører til ansvar?
Forståelse af CSA	X is a kind of Y	Hvilke forståelser findes?
Slags af trusler	X is a kind of Y	Hvad er de forskellige slags trusler?
Slags af træningsmetoder	X is a kind Y	Hvilke slags træningsmetoder findes?

Tabel 3.2: Identificerede domæner - egen tilvirkning

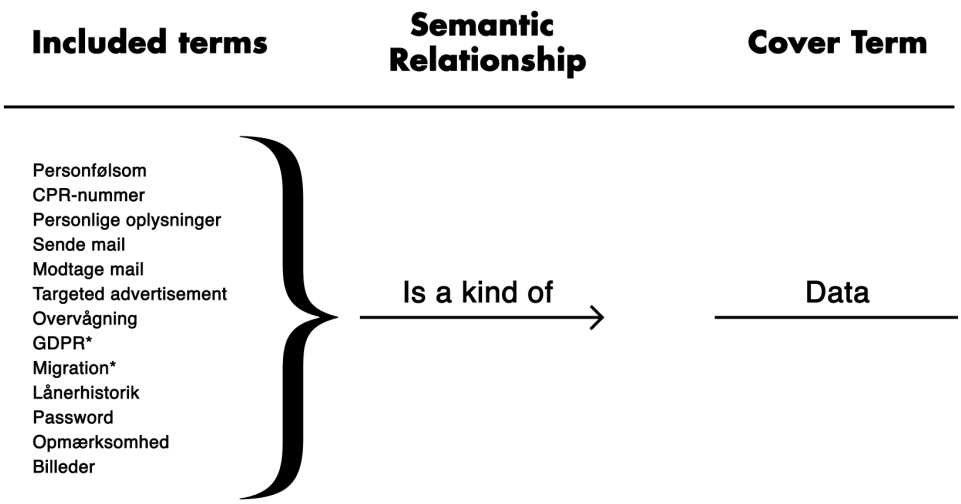
Nu hvor dette er blevet præsenteret, hvad betyder disse domæner så?

Domænernes betydning

I den følgende analyse, vil hvert identificeret domæne analyseres enkeltvis. Herefter vil følge en opsamling omkring alle domænerne med henblik på at vise, hvad disse domæner så fortæller om kulturen omkring CSA i Hjørring Kommune.

Data

Dette segment indeholder, hvordan interviewpersonerne snakkede om data. Figur 3.5 viser, hvordan J. P. Spradley (1979)'s arbejdsark blev udfyldt med dataen fra interviewene. Dette segment er navngivet *data*, da de inkluderede termer udtrukket fra interviewene og konteksten ordene blev sagt i, alle var en slags data. Data blev derfor til et cover term. Dette gør at de inkluderede termer er en striks inklusion - altså "en slags af"



Figur 3.5: Semantisk relation - Data domæne - egen tilvirkning

Da Hjørring Kommune hovedsageligt arbejder med personfølsomme oplysninger, er det et af de mest repræsenterede termer brugt i forbindelse med beskrivelser af data.
En skolelærer udtaler følgende:

> *"Men det handler også om, at der er nogen, der tager ansvar for at få fulgt op på det og sørge for, at sikkerheden er i orden"*
> (Skolelærer - Bilag 1, 01:55 [1.2])

Dette var i forbindelse med hans uddybelse af de tre ord han forbinder med cybersecurity i starten af interviewet. Hans tre ord var: sikkerhed, ansvar og forebyggelse. Her nævner han altså, at han har en direkte forbindelse med håndteringen af dataen, hvilke personer som tager ansvar, samt at sikkerheden er "i orden". I og med, at ordvalget i dette citat er mere abstrakt tyder det på, at han forventer, at en række praksisser og politikker er til stede for at kunne opnå det rette sikkerhedsniveau.

Når han så efterfølgende bliver spurgt ind til disse normer og ansvar, i forbindelse med CSA og bliver spurgt direkte ind til, om hans kollegaer oftest tænker, at IT-afdelingen har ansvaret for dette, og hvordan hans kollegaers indstilling til subjektet er, svarer han følgende:

> *"Det tror jeg, der er mange her, der gør. Jeg tror, der er mange, der tænker, at vores IT-mand, han styrer det der. Faktisk. Det er nok de 80 procent, der er, som jeg nævnte før"*
> (Skolelærer - Bilag 1, 07:36 [1.8])

Her kommer det til syne, at kulturen på hans arbejdsplads er at fralægge sig ansvaret i forhold til CSA, fordi perspektivet fra hans kollegaer er at "Jeg tror, der er mange, der tænker, at vores IT-mand, han styrer det". Dette kan tyde på, at, fordi det omhandler IT, så er det ikke en del af lærernes fagområde, som derfor ikke ser det som en af deres kerneopgaver. Dette er nødvendigvis ikke årsagen, da CSA er et paradoks, hvor man ikke behøver at forstå årsagerne til handlingerne, angrebenes natur eller de ondsindede aktørers intentioner. På trods af dette kan man gennem de rigtige praksisser undgå langt de fleste tilfælde af angreb. Når lærerne arbejder med børnenes personfølsomme oplysninger, kan det argumenteres for, at deres sikkerhed faktisk er en kerneopgave for lærerne i dette tilfælde. Empirien viser dog her, at det er vanerne og det kendte, der bliver lagt fokus på, både i forbindelse med undervisningen, men også i forbindelse med deres egne handlinger, når det kommer til CSA ansvar. Dette fænomen genkender en afdelingsleder i handicapområdet også:

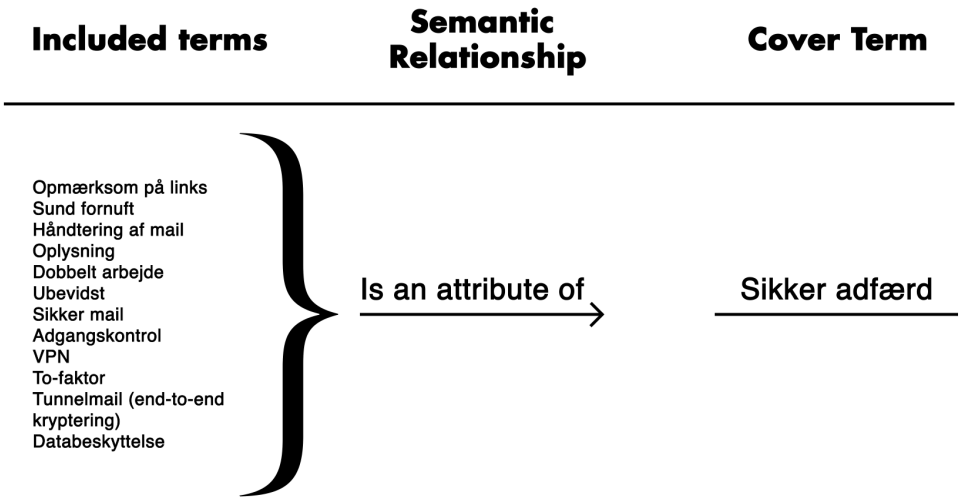
> *"(...) når jeg får sådan en (phishing mail) så sender jeg den til IT, fordi det regner jeg med at mine kolleger også gør, så hvis der er et mønster, så samler de det og sender ud, hvis vi skal være opmærksomme på det. Det er dem der har den der sammenhængskraft for alle os, der er ansat i kommunen."*
> (Afdelingsleder, Handicapområdet - Bilag 2, 17:33 [2.12])

Dog nævner vedkommende også årsagen til handlingen. Her erkender hun, at IT-afdelingen har det overordnede overblik, hvilket er årsagen til hendes handling, men nævner ikke noget om hendes personlige ansvar.

Dette domæne viser altså, at der håndteres en del data i Hjørring Kommune - også en del personfølsom data. Som analysen viser, lader det til, at der på tværs af afdelinger er en kultur omkring, at organisationen er meget opdelt i de her afdelinger. På tværs af afdelinger er der en mening omkring, at når det handler om IT, så er det IT-afdelingens ansvar.

Sikker adfærd

Dette segment undersøger domænet kaldet *sikker adfærd* inden for CSA hos Hjørring Kommunes medarbejdere. Figur 3.6 viser den semantiske relation som dette domæne bygger på. Dette domæne opstod da empirien viste en masse udsagn, der var en egenskab ved sikker adfærd. Disse blev altså til included terms for cover term'et *sikker adfærd*.



Figur 3.6: Semantisk relation - Sikker adfærd domæne - egen tilvirkning

I forbindelse med, at Hjørring Kommune hovedsageligt arbejder med personfølsomme data, hvilket også er tilfældet for alle kommuner, er det relevant at undersøge, hvilke udsagn medarbejderne bruger til at beskrive deres forståelse inden for dette, samt deres adfærd inden for dette domæne.

Udsagn som "opmærksom på links", "sund fornuft"og "oplysning"viser kulturens indvirkning på den sikre adfærd hos medarbejderne. Et eksempel er når det kommer til sikker mail. Her udtaler en demenskonsulent følgende:

> *"Det første, det er, at jeg tænker, at være sikker at mail, og dele personlige oplysninger. Og så tænker jeg også det der, når jeg får noget ind i min inbox, hvad jeg siger ja til? Hvad hedder det? Skal jeg bare skrive det, som jeg har samtidigt tænkt på? Hvad accepterer jeg i min inbox?"*
> (Demenskonsulent - Bilag 3, 01:35 [3.1])

Her nævner hun også opmærksomheden i forbindelse med phishing-angreb, og hvad hendes tanker er når sådanne mails rammer hendes inbox. Bibliotekaren sætter nogle ord på deres infrastruktur og, hvordan setuppet er omkring sikkerheden:

> *"Ja, altså man kan sige, vi har jo ikke dataen som sådan, man kan ikke gå ned og stjæle en computer nede ved os og så har man alle vores låneroplysninger, det kan man ikke, så er det mere den daglige drift, altså håndteringen af det, og det synes jeg er top vigtigt. Så kan man sige at IT afdelingen, det er mere infrastrukturen på en eller anden måde, de har jo ikke håndteringen af dataen som sådan, men det er mere sådan at de har lavet et ordentligt system nede hos os håber jeg."*
> (Bibliotekar - Bilag 4, 29:28 [4.25])

Ordvalget brugt af bibliotekaren her tyder på et håb om at IT-afdelingen har lavet et godt stykke arbejde, samt at alt dataen ligger i cloud løsninger som forhøjer deres håndtering af de personlige

oplysninger de arbejder med og dermed deres sikre adfærd. En medarbejder fra databeskyttelsesteamet erkender også, at der er mange forskellige forståelser i organisationen, hvilket skaber udfordringer de steder, hvor CSA ikke er en primær arbejdsopgave i deres stilling (Se bilag A.6). For at få mere og bedre handling fra medarbejderne erkender medarbejderen i databeskyttelsesteamet også, at oplysning af cybersecurity er vigtigt, men understreger i særdeleshed værdien af CSA, da det ikke er noget de fleste i organisationen mærker en direkte værdi fra i forbindelse med deres arbejdsdag (Se bilag A.6). Den usynlige værdi som CSA skaber i virksomheder er svært at kvantificere, da der ikke er lavet direkte modeller, metoder eller metodologier til at måle CSA, både på individuelt plan og på tværs af organisationer.
Udsagn fra empirien viser dog, at alle respondenterne finder CSA vigtigt.

Da bibliotekaren blev spurgt ind til om han havde undersøgt, hvor meget adgang han havde i systemerne var det uvist for ham, da han bare forventede, at de rette begrænsninger var sat op:

> *"Ja, altså det er jo så heldigvis, kan man sige, begrænset, jeg er faktisk ikke engang selv helt klar over, hvor meget data jeg har adgang til, fordi jeg har ikke undersøgt, lad os se hvor langt vi kan gå ud på drevet, jeg har ikke gået i gang med den øvelse, men jeg går ud fra og håber på at der er nogen nede i IT, som har sat nogle begrænsninger op på mig og på min bruger, på hvor galt det ligesom kan gå."*
> (Bibliotekar - Bilag 4, 19:17 [4.15])

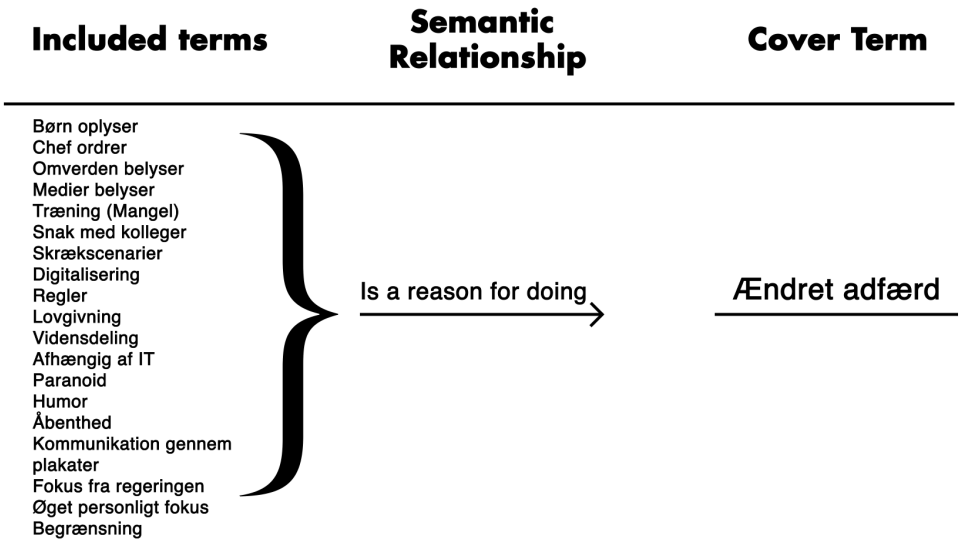
I forlængelse af dette uddyber bibliotekaren:

> *"Ja, det kan man godt sige på den måde, men det er også en almindelig driftssituation, Martin er ansat på biblioteket, han skal have adgang til de her mapper og han skal have adgang til de her systemer, det synes jeg er en meget logisk måde at lave det på. Det er det samme når jeg sidder og laver hjemmesider og jeg skal give adgang til en af jer, så får du redaktøradgang og så skal jeg nok sørge for at du ikke kan pille inde i coren af et eller andet dopa system eller sådan noget i den stil, det skal jeg nok selv gøre."*
> (Bibliotekar - Bilag 4, 19:59 [4.16])

Dette korresponderer med forventningerne til IT-afdelingen fra det tidligere afsnit 3.2.1, at kulturen på nuværende tidspunkt viser at lade meget af ansvaret ende på bordet hos IT-afdelingen. Dette er modsigende i forhold til, hvad medarbejderen i databeskyttelsesteamet ønsker, da hun mener at CSA skal indlejres i kulturen hos de enkelte individer, hvor hun specifikt nævner, at det ikke blot er en opgave for IT-afdelingen, men et fælles ansvar for at højne CSA niveauet på tværs af organisationen. Endvidere mener hun dog, at IT-afdelingen skal være bedre til at få alle med (Se bilag A.6).
Kulturen omkring sikker adfærd lader altså til at være, at gøre IT-afdelingen opmærksom på hændelser, phishing-mails eller lignende.

Ændret adfærd

Dette segment undersøger domænet om *ændret adfærd* i forbindelse med CSA hos medarbejderne i Hjørring Kommune, og den tilgang de har til at få den ønskede ændring hos medarbejderne. Figur 3.7 viser J. P. Spradley (1979)s arbejdsark udfyldt. Ændret adfærd domænet blev valgt, da de udvalgte inkluderede termer og konteksten de ord blev brugt i under interviewene var en rationale for cover term'et *ændret adfærd*. Udsagnene i included terms er altså "a reason for doing"ændret adfærd. Denne ændrede adfærd er endemålet med CSA, hvorfor det er relevant, at det kommer til syne i empirien.



Figur 3.7: Semantisk relation - Ændret adfærd domæne - egen tilvirkning

I forhold til vigtigheden nævner skolelæreren, at han mener det er "enormt vigtigt", ikke kun i forhold til CSA, men også at begå sig på internettet:

> *"For mit vedkommende ja. (...) Og det er noget, jeg tager fat i af og til. Men det er ikke noget, der sådan fastlagt (...) ligger i nogen former. For årsplaner eller noget som helst. Så det er noget, jeg tænker, man skal selv have lysten til. Ligesom at tage det op med klassen. Men jeg synes jo, det er enormt vigtigt. Fordi som du selv siger, internettet er bare et farligt sted. Men det er ikke noget, alle gør langt fra. Jeg tror heller ikke, det er ret mange her på stedet, der tager det op. I deres undervisning aktivt. Selvom det er enormt vigtigt."*
> (Skolelærer - Bilag 1, 10:35 [1.12])

Ordene som skolelæreren vælger at bruge her, er at gøre det uspecifikt og fokusere mere på lysten til at tage det op, som et emne lærerne selv skal vurdere om det har vigtigheden til at blive en aktiv del af undervisningen. At lysten styrer det, gør det nemt at undgå for lærere som ikke er IT kyndige, hvorpå de måske hellere ser vigtigheden indenfor andre emner, selvom en stor del af både lærerne og børnenes aktive tid bliver brugt på internettet, hvormed der kan argumenteres for,

at det skal have en større repræsentation på bredt plan. Her bliver ansvaret igen påtalt, intuitivt, ved planlægningen af undervisningen.

Når det kommer til informationen og oplysningerne om CSA, kommer det ikke kun fra ledelsen i Hjørring kommune. Demenskonsulenten nævner, at hun har fået værdifuld viden fra hendes børn:

> *"Det er noget, jeg får at vide af mine børn, jeg skal. Altså, nogen siger bare, bare tryk OK til det hele, ikke også, og andre de siger, pas lige på. Hvad er det, du trykker på, og klikker på, og hvis det er noget, du er usikker på og sådan noget, så ja. Jeg får jo nogle gange nogle mails om, at på min arbejdsmail, du har ikke hentet den og den pakke, eller du har vundet et eller andet, hvor jeg tænker, det skal jeg i hvert fald ikke lige klikke på, fordi det er helt sikkert, for jeg har ikke bestilt nogen pakke over mit arbejdsmail, så det er i hvert fald ikke noget, jeg lige. . . "*
> (Demenskonsulent - Bilag 3, 03:04 [3.3])

Demenskonsulenten viser her, at det er muligt midlertidigt at ændre adfærd, ved at indføre regler eller politikker, men som tidligere beskrevet vil en ændring i forståelsen hos medarbejderen være nødvendig for at skabe en reel ændring i adfærden.

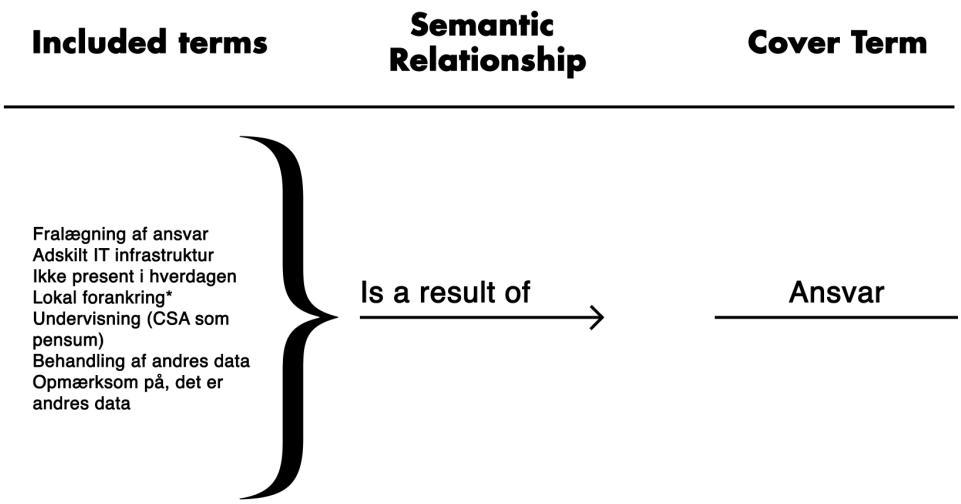
Der er også en enighed mellem afdelingslederen og en medarbejder fra databeskyttelsesteamet, om at de foretrækker at give en gulerod frem for pisken (Se bilag A.6 og A.7. Medarbejderen fra databeskyttelsesteamet nævner, at guleroden kan forekomme gennem humor og ros når bruddet bliver anmeldt (Se bilag A.6). Afdelingslederen giver gulerødder ved, igen, at bruge humor, være åben og i fællesskab finde en løsning på et givent problem. Her nævner hun også, at de før i tiden gav slikposer ud, for at hjælpe medarbejderne med at huske på forskellige tiltag, hvor cybersecurity og CSA blev nævnt som eksempler (Se bilag A.7).

En strategi som databeskyttelsesteamet bruger, er den ene generelt bærer "nej-hatten", hvor den anden har en mere positiv tilgang, hvilket, ifølge hende, skaber en succesfuld dynamik i forhold til at tilføje nye tiltag og opretholde tiltag i forbindelse med CSA (Se bilag A.5). Idéen med dette, er, at det skaber en tryghed for medarbejderne at gå til databeskyttelsesteamet eller IT-afdelingen x med potentielle løsninger, som de så kan drøfte i fællesskab i databeskyttelsesteamet (Se bilag A.6). Endvidere nævner den ene medarbejder i databeskyttelse, at hvis der er forslag som ikke kan tilføjes eller afslåes, finder de en fælles løsning på problemet som kan overholde diverse restriktioner for at sikre cybersikkerheden (Se bilag A.6)

Kulturen for at ændre medarbejdernes adfærd i Hjørring Kommune har fokus på åbenhed, humor og konceptet med at give en gulerod fremfor pisken. Denne metode har til fordel at italesætte emnet, hvilket kan tænkes at det bliver mere håndgribeligt for medarbejderne. Dette gør også, at medarbejderne har en mere åben tilgang til CSA og et øget fokus til CSA når det kommer til deres arbejdsdag, selvom de måske mener det ligger perifert i forhold til deres normale arbejdsopgaver.

Ansvar

Dette segment undersøger domænet, der kaldes *ansvar*, som er en forårsaget virkning fra de inkluderede termer. Figur 3.8 viser J. P. Spradley (1979)'s udfyldte arbejdsark. Ansvar er et af hovedområderne når det kommer til CSA og den misforståelse som ofte forekommer, hvilket gør det til et naturligt domæne i forbindelse med dette projekt. Derfor er det relevant, at dette også kom til syne i empirien i denne undersøgelse.



Figur 3.8: Semantisk relation - Ansvar Domæne - egen tilvirkning

Termer som fralægning af ansvar og behandling af andres data er uddybet nærmere i de tidligere afsnit. Når det kommer til adskilt IT infrastruktur nævner bibliotekaren følgende:

> *"Ja, man kan sige beskyttelsen udadtil, den er todelt hos os, fordi vi har jo ligesom, vi har en IT infrastruktur hos os, men den er ude i en armslængdeprincip fordi at vores infrastruktur, altså i huset, den bliver lavet hernede et eller andet sted, vi bor jo et andet sted, så det er lidt distanceret på en eller anden måde, det er ikke sådan noget vi, det er meget kommunalt ikke, det er noget IT de tager sig af, det fikser de nok, det er sådan den ene del af det. . . "*
> (Bibliotekar - Bilag 4, 09:07 [4.7])

Her nævner han specifikt, at beskyttelsen er todelt, hvor den ene er i et "armslængdeprincip", som IT-afdelingen står for. Når han refererer til, at "det bliver lavet hernede", refererer han til rådhuset i Hjørring, hvor interviewet foregik. Dette betyder, at biblioteket ikke har den store indflydelse på første del af beskyttelsen, hvorimod den anden del beskrives yderligere herunder:

> *"...Men så har vi så vores, hvad hedder det, vores fagsystem, vores biblioteksystem, vores hjemmeside drift og det er ligesom, det kører et andet sted fra, så det er sådan, jeg tror måske nok det måske er en lidt usund tankemæssigt at det er distanceret og ikke er noget vi selv har styr på, men samtidigt med så ved jeg at dem som sidder i den anden ende og tager sig af det, de har markant mere styr på det, altså vi har ikke ressourcer til at have IT personale der kan styre sådan noget, men det gør måske også lidt at sådan tankesæt mæssigt, så er det ikke så present i hverdagen, der er styr på det regner vi med."*
> (Bibliotekar - Bilag 4, 09:07 [4.7])

I denne anden del, forklarer bibliotekaren, bliver sikkerheden håndteret af en anden gruppe mennesker, mens de ansatte er brugere af systemet. Begrundelsen lyder på, at de ikke har nok ressourcer til at have IT personale til at styre den sikkerhed. Derudover nævner bibliotekaren, at CSA ikke er fremtrædent i hverdagen, samt at distanceringen ikke skaber et sundt tankemæssigt forhold til sikkerheden. Dette kan skabe en naturlig modstand i kulturen i forbindelse med implementering eller oplysning af CSA hos medarbejderne, da distancen kan give dem forståelsen at det ikke er en del af deres daglige arbejdsopgaver.

Der bliver sået små frø i baghovedet på medarbejdere, efter en fra databeskyttelsesteamet har haft en dialog med medarbejderne, hvor det normalt ikke bliver bragt op ellers ifølge bibliotekaren:

> *"(...) Men altså, det er sådan noget man kan se blive bedre, for når vi så har haft besøg af Ulla (red. en fra databeskyttelse teamet) for eksempel og det bliver italesat, så har man det måske i en, det er måske ikke det man snakker over hver dag over frokosten, men at det ligesom er, at der er et frø som er sået og så kunne jeg godt, jeg er sådan lidt firkantet, så jeg kunne godt tænke mig at vi siger fra på onsdag låser alle kraftædeme deres computere og låser også andres når de går forbi den, men sådan fungerer virkeligheden bare ikke, det tager tid og gøde den her awareness åbenbart ikke."*
> (Bibliotekar - Bilag 4, 23:00 [4.19])

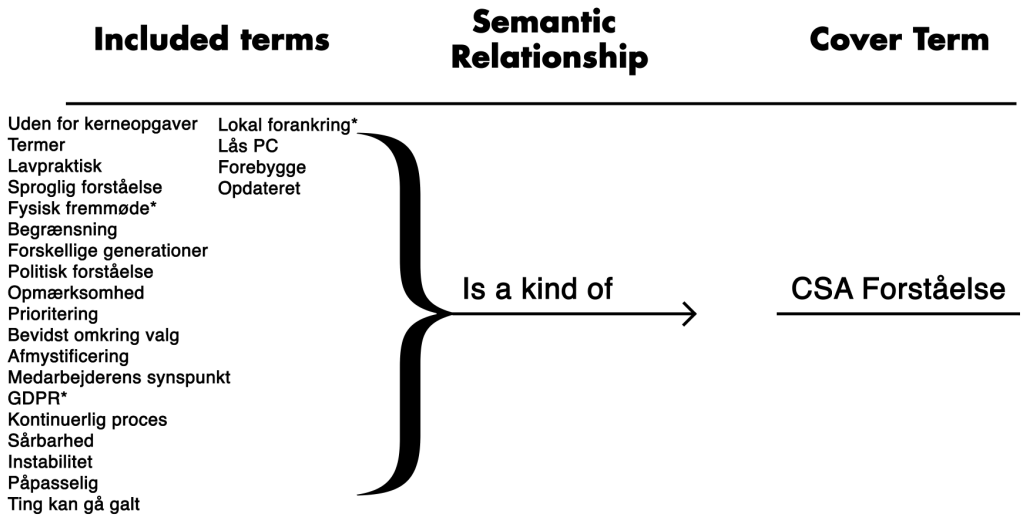
Dette stemmer overens med den filosofi og strategi som medarbejderen i databeskyttelse og afdelingslederen i sekretariatet fortæller i rekonstruktionen, som humor og åbenhed (Se bilag A.6 og A.7. Ydermere understreger bibliotekaren også, at det er andre personers data de arbejder med, og sammenligner det med, at man skal behandle det, som en mekaniker ville behandle en kundes bil:

> *"(...) Det ville være det samme hvis jeg var en mekaniker og nogen kom og afleverede deres bil, så passer jeg også på den, altså på den måde ikke..."* (Bibliotekar - Bilag 4, 21:25 [4.18])

Denne tankegang viser, at der alligevel er en form for ansvarsfølelse hos medarbejderne i forhold til behandligen af andres data. Denne ansvarsfølelse kan ses som målet for CSA, da der i så fald er større chance for en sikker adfærd i forhold til behandlingen af data.

CSA forståelse

Dette afsnit undersøger domænet *CSA forståelse*, som er en forårsaget virkning af de inkluderede termer. Figur 3.9 viser J. P. Spradley (1979)'s udfyldte arbejdsark. CSA forståelse blev identificeret som domæne, da det er et af de største punkter, hvor der sker misalignment hos medarbejdere, og på tværs af virksomheder (Hoeing m.fl., 2022). Analysen for 3.1 undersøgte de individuelle personer, grupper og områder, som danner den nuværende forståelse hos Hjørring Kommune. Dette segment har til formål at undersøge det kulturelle aspekt for organisationen indenfor dette domæne.



Figur 3.9: Semantisk relation - CSA forståelse domæne - egen tilvirkning

Mange af de inkluderede termer er nævnt i tidligere afsnit, hvor specifikt sproglig forståelse, fysisk fremmøde og opmærksomhed på CSA er nævneværdige i forbindelse med kulturen hos Hjørring Kommune, specielt i forbindelse med filosofien og strategierne hos medarbejderen i databeskyttelse og afdelingslederen i sekretariatet (Se bilag A.6 og A.7.

Både skolelæreren, bibliotekaren, projektlederne og databeskyttelsesteamet er i kongruens i forbindelse med, at løsningerne for CSA skal være lavpraktiske og give mening for at kunne passe ind i kulturen hos Hjørring Kommune, selvom det ikke er et emne som ofte er italesat i hverdagen.

> *"I hverdagen tænker jeg ikke ret meget over det. Jo, på helt lavpraktisk niveau, tænker jeg over det. ugh, jeg er begyndt at afvise cookies, fordi jeg tænker sådan, det skal man nok. Man gør det sådan lidt hovedløst, indtil jeg fandt ud af, jeg får det samme ind på mine medier. Men jeg gør det lidt hovedløst. Desværre."*
> (Afdelingsleder, Handicapområdet - Bilag 2, 08:29 [2.7])

Der viste sig også en inkongruens hos nogle af medarbejderne, som sammenlignede CSA med målrettede reklamer og cookies, hvilket viser et vist niveau af teknologisk forståelse. Dette blev

uddybet i afsnit 3.1. En projektleder nævner specifikt, at sikkerhedshændelser og CSA ikke er noget de generelt tager op på ledermøder, medmindre det kommer "oppefra":

> *"Altså sådan en historie har jeg fortalt fordi den er skideskæg, men det er ikke sådan at vi på ledermøder for eksempel lige drøfter er vi udfordret på noget sikkerhedsmæssigt. Det gør vi ikke. Så er det noget, der kommer oppe fra. I skal være opmærksomme på et eller andet, eller fra IT. Så er det noget vi skal forholde os til og så gør vi så det. Men det er ikke sådan at vi har jævnlige møder om vi overholder det ene og det andet."*
> (Afdelingsleder, Handicapområdet - Bilag 2, 20:58 [2.14])

Med "oppefra" mener afdelingslederen her, at det er information som kommer fra databeskyttelsesteamet eller højere ledelseslag. Når det kommer til behandling af data forklarer bibliotekaren, hvordan de bearbejder det, hvordan det bliver opbevaret, sendt og, hvordan kommunikation mellem andre biblioteker sker:

> *"Altså, hvordan det fungerer i vores fagsystem? Altså det bliver sendt krypteret i hvert fald og vi har det ikke som sådan, vi har sådan et datapoint vi har der ligger et eller andet sted, hvor vores fagsystem kan kigge ned i gennem en sikker forbindelse, det cirka så meget jeg ved om det. Jamen også sådan noget som sendt frem og tilbage, for så er det nemlig den der, vi arbejder i to. Vi har sådan et fagsystem vi arbejder i, men hvis vi skal sende bestillinger til andre biblioteker, så skal man ud af det og så over i et andet krypteret system, men det er så der man har muligheden for at for eksempel sende CPR nummer, det er ikke noget, der er potentielt nogen som kan få fat i det, men det er der, hvor man skal vælge de her lånernumre, men hvordan det bliver sendt og sådan noget, jeg går ud fra at der er styr på sikkerheden, men jeg ved det ikke sådan helt konkret."*
> (Bibliotekar - Bilag 4, 28:09 [4.24])

Her viser bibliotekaren en forståelse af, hvordan systemet virker. Dette er også tilfældet når det kommer til projektlederne. De er også bevidste om, at de ikke er eksperter indenfor området, hvor kulturen giver medarbejderne råderum og mulighed for at spørge om hjælp uden at blive dømt. Ydermere, forklarer bibliotekaren, at CSA er særdeles vigtigt når de står i udlån og låner bøger til borgere:

> *"Altså helt lavpraktisk i min arbejdsdag, lige om lidt når jeg er færdig med at snakke med jer, så skal jeg jo ned og passe biblioteket altså ude i udlån, og der er det en del af det, for der står man jo med, inde i systemet, men ude i et offentligt rum. Det er sådan noget, det tænker jeg i hvert fald over, når man arbejder med det også, vi har en meget meget åbent bibliotek, vi har nede hos os, folk kan kigge med sådan inde over skulderen og sådan noget, ja også sådan noget med, hvad man sender til folk. For der bliver bare sendt utroligt meget mellem biblioteker, vi har sådan noget interubant samarbejde og hvad der bliver sendt der, det er især der hvor vi passer på synes jeg."*
> (Bibliotekar - Bilag 4, 32:21 [4.27])

Her understreger bibliotekaren, at de står i et offentligt rum, hvilket gør at de er mere sårbare der, da de besøgende gæster kan se skærmen som bibliotekaren arbejder på, hvor både forståelsen og ansvaret er særdeles i fokus. Ydermere, nævner afdelingslederen i sekretariatet at sproget er

en vital del til at få forståelsen alignet hos medarbejderne i kommunen og mener, at sproget og kulturen går hånd i hånd, som skal tilpasses til det personel som man arbejder med. Dette stemmer overens med fundene i litteraturstudiet (Hoeing m.fl., 2022).

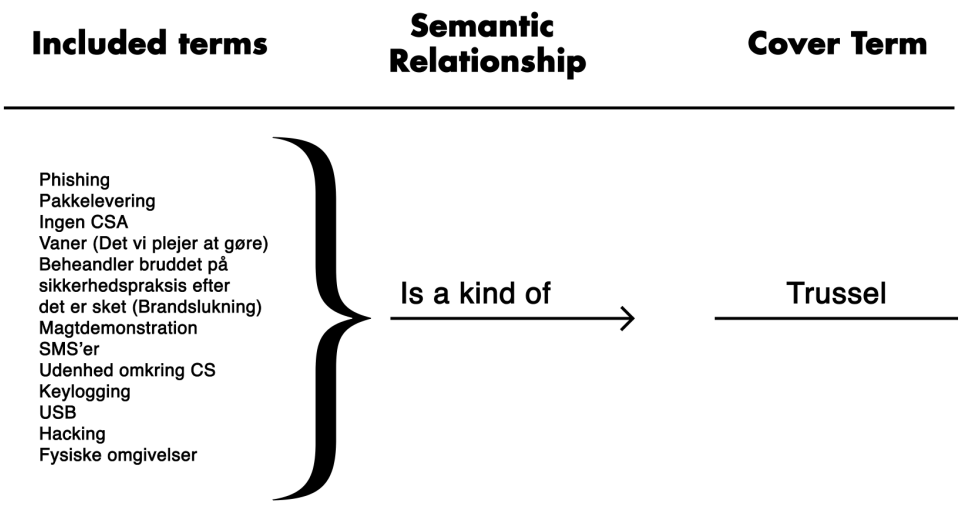
GDPR har haft en lovmæssig indflydelse på opstramningen af persondata, hvilket bibliotekaren nævner, at han har kunnet mærke det i hans arbejdsdag:

> *"Ja, hvis vi tager dem en ad gangen, GDPR det er bare sådan noget jeg kan mærke, jeg har været i biblioteksbranchen i nogle år og det er bare sådan noget, hvor der bare er blevet skruet på en knap, hvor man lige pludselig er kommet i tanker om, hov det kan måske være vi sidder, altså vi er bare et bibliotek, men vi har måske adgang til nogle systemer, noget data som er følsom for nogen, det er sådan den ene del af det, det er noget jeg kan mærke er blevet eskaleret."*
> (Bibliotekar - Bilag 4, 02:09 [4.2])

Der er en generel konsensus om forståelsen af vigtigheden af CSA i Hjørring Kommune, hvor de anerkender vigtigheden af det, samt deres mangel af både viden og påtalelsen af emnet i hverdagen, samt i møder. Den lovmæssige vinkel, ved den tvungne implementering af GDPR, anerkender interviewpersonerne også har forhøjet deres viden angående vigtigheden af persondata. Dette har ligeledes hjulpet dem til en højere forståelse af CSA, dog accepterer de, at de ikke er i mål endnu, i forbindelse med deres forståelse af CSA, da det er en kontinuerlig proces.

Trussel

Dette segment har domænet *trussel* i fokus. Figur 3.10 viser J. P. Spradley (1979)'s udfyldte arbejdsark. De inkluderede termer er de udsagn som interviewpersonerne brugte, da de blev spurgt ind til angrebsformer og ondsindede aktører.



Figur 3.10: Semantisk relation - Trussel domæne - egen tilvirkning

En medarbejder fra databeskyttelsesteamet anerkender, at medarbejderne ved, at der findes forskellige trusler, som kan ses i figur 3.10, eksempelvis keylogging og phishing, hvor phishing er det mest presserende angreb på globalt niveau (Hoeing m.fl., 2022):

> *"Altså, nu ved de godt, hvad en phishing-mail er. De ved, hvad det er, og de ved, hvad man skal og ikke skal gøre. Nu er de nået over begynderniveauet. Nu skal vi lige have dem på mellemniveau. Og det er det, vi springer i gang med at tage. Og det er svært at lave noget for alle."*
> (Medarbejder i databeskyttelsesteam - Bilag 5, 05:27 [5.4])

Kulturmæssigt har empirien nævnt, at deres metodologi er effektiv, hvilket betyder at, hvis de fortsætter med at have fokus på åbenhed, humor og lavpraktiske løsninger, vil den generelle medarbejder få et højere niveau og blive mere resistente imod trusler. Bibliotekaren anerkender, at CSA ikke er en løsning som giver et facit, men at det er en kontinuerlig proces:

> *"Jamen jeg tror, jeg mener faktisk lidt det som jeg, det man kan sige med processen, at man ikke er færdig, man kan ligesom godt tænke at vi er dækket af, at vi sådan har brandsikret eller prøvet sådan at fremtidssikre os lidt mod eller andet, men der er jo bare, der sidder bare nogle kloge mennesker et eller andet sted med nogle rimelig trælse hensigter også, som nok skal komme videre end det. . . "*
> (Bibliotekar - Bilag 4, 04:30 [4.4])

Denne opfattelse af den kontinuerlige proces er ligeledes delt med medarbejderne i databeskyttelsesteamet (Se bilag A.6). "Brandslukning"-termet i citatet bliver brugt som forståelse af, at der først bliver reageret efter der har været et brud. Bibliotekaren nævner, at de prøver så vidt muligt at fremtidssikre sig, men denne forecasting er oftest ikke mulig i visse dele i organisationen, da vigtigheden, forståelsen og ansvaret er inkongruent. Selvom kulturen er tilpasset organisationens personel, så er denne brandslukning en naturlig effekt af medarbejderes mangel på viden, ansvarsbevidsthed eller konsekvenserne ved et brud. Ydermere, nævner bibliotekaren, at keylogging og USB adgang er områder de har direkte politikker omkring, for at have de rigtige aktioner i de tilfælde situationerne opstår:

> *"Mmm, ja, altså hvis man nu tager udgangspunkt i de her ting for eksempel (hans tre punkter), nu tager vi keylogging, altså der har vi haft, der er rigtig mange mennesker som bruger biblioteket som en print central, hvor man går ned og printer fordi det ikke kan betale sig at have en printer derhjemme, men vi har lukket af for alle vores USB porte, fordi det er ligesom den primære adgang til keylogging. (...) så bliver man lige pludselig meget bevidst om når folk kommer med deres USB pinde og siger "Kan jeg få det her ud", nej det kan du ikke. Der bliver det ligesom inkorporeret i en hverdag der fungerer på en eller anden måde, men også tilstedekommer noget brok og diskussioner, noget med publikumservice, altså det der med, det plejer vi jo at kunne og det kan vi lige pludselig ikke længere, ergo serviceforringelse sådan noget i den stil. . . "*
> (Bibliotekar - Bilag 4, 07:03 [4.6])

Bibliotekaren anerkender, at biblioteket oftest er en printcentral, og da der er lukkede USB porte, og de har en police med ikke at indsætte USB'er ind i PC'erne, bliver det en fast del af deres hverdag at forklare hvorfor det ikke er muligt at anvende USB-stik, da situationen ofte opstår. Dette gør, at

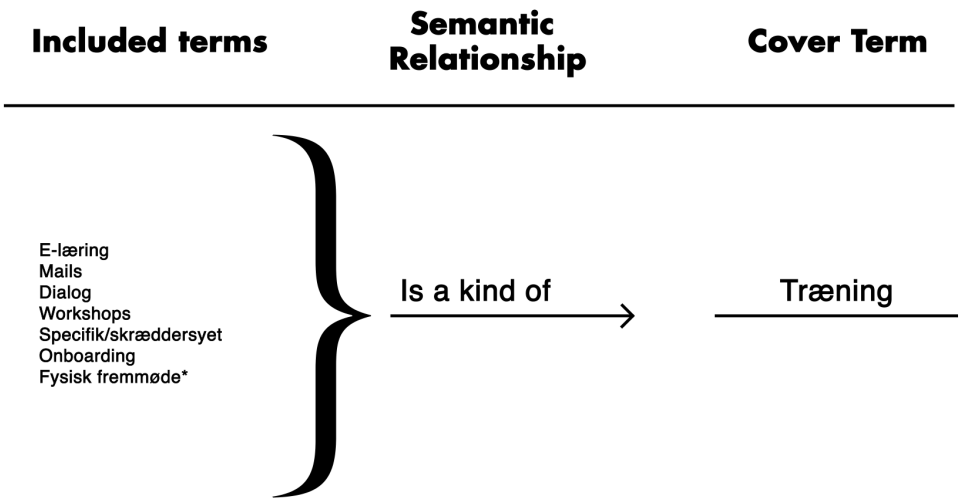
medarbejderne er forberedte på, hvad de skal gøre i de tilfælde, hvor situationen opstår, med støtte fra policerne. Dette viser, at bibliotekerne i Hjørring har taget i mente de presserende situationer som kan opstå, og have direkte handlinger til at modarbejde dette, selvom det kan give en forringet service til brugerne af biblioteket. USB-pinde er kvantificerbart, og en generel kendt teknologi som har et fysisk element til sig, hvor der kan argumenteres for at det er en af årsagerne til at det er mere håndgribeligt at lave policer og handleplaner for situationerne som opstår. På bredt plan vil frekvensen af eksempelvis USB situationer og phishing mails, vil phishing være væsentligt mere repræsentativt. I og med phishing mails ikke er kvantificerbart er det et væsentligt sværere område at lave policer omkring, da det kræver både viden, ansvar og teknologisk forståelse på et andet niveau end at fjerne adgang til USB porte på offentlige computere og ikke indsætte USB'er i deres arbejds pc'er. Denne opstramning af specifikt keylogging og USB tilgang er steget efter der har været uheldige sager i biblioteksbranchen:

> *"Og så keylogging, det er fordi der har været i vores branche nogle mega uheldige sager lige nøjagtigt med det, det er sådan noget vi har brugt mange timer over at tænke på hvordan man håndterer sådan noget, på en meget lavpraktisk måde som også kan fungere i hverdagen. Og så hacking det er fordi jeg sidder med hjemmesider, sociale medier og sådan noget, og det er bare, det er sådan noget jeg tænker på en gang imellem. Og hvor der også, jeg sidder med i sådan nogle nationale netværk, hvor man kan se kolleger i andre kommuner, hvor de bare sådan mister det hele, så ja."*
> (Bibliotekar - Bilag 4, 02:09 [4.2])

Denne kendskab til tidligere branchespecifikke angreb giver anledning til at reagere eller agere på de kendte trusler. På den måde er det nødvendigt at kende til truslerne, før det er muligt at gøre noget ved dem. Her har databeskyttelsesteamet en opgave i at indsamle information om trusselsbilledet i kommunen, og videreformidle dette til de relevante afdelinger i kommunen.
Brandsluknings-princippet viser også at Hjørring Kommune er omstillingsparate og intuitivt accepterer konceptet om, at det ikke handler om hvorvidt man bliver hacket, men om hvornår det sker.

Træning

Dette segment undersøger *træning*-domænet, som er en forårsaget virkning fra de inkluderede termer. Figur 3.11 viser J. P. Spradley (1979)'s udfyldte arbejdsark. Træning blev valgt, da det er et af de bedste former for forebyggelse for angreb og uddannelse af medarbejdere.



Figur 3.11: Semantisk relation - Træning domæne - egen tilvirkning

Generelt får medarbejderne ikke træning indenfor CSA, som demenskonsulent uddyber på:

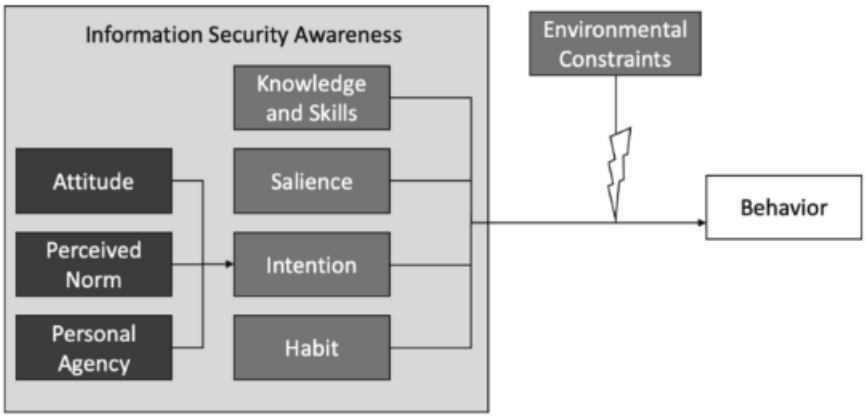
> *"Ikke sådan lige, nej. Det er som, hvad man ellers finder ud af gennem tiden. Ja, der skal man ikke sende hen, og der kan man godt sende hen, og ja, så må man jo så spørge et eller andet sted."*
> (Demenskonsulent - Bilag 3, 08:45 [3.8])

En medarbejder i databeskyttelsesteamet accepterer deres nuværende niveau af CSA, hvor hun nævner at på bredt plan har medarbejderne kendskab til phishing-angreb, hvorfor det ville være naturligt at deres næste mål er at videreudvikle dette til flere former for angreb og udbrede den viden (Se bilag A.5).

Det kan ses, at træning i CSA, kan være et middel til at øge kendskaben til CSA blandt medarbejdere i Hjørring Kommune. Den eksisterende litteratur viser, at træning kan være et fordelagtigt værktøj, hvorfor det ligeledes kunne være en fordel at indføre jævnlige træninger som en del af kulturen i kommunen.

3.3 Konteksten af modenhed omkring CSA

For at dykke dybere ned konteksten for CSA i Hjørring Kommune og indsatsen på awareness området, benyttes der i denne analysedel en tidligere beskrevet modenhedsmodel fra Fertig m.fl. (2020), se figur 3.12. Dette afsnit vil undersøge modenheden indenfor CSA i forhold til at ændre adfærd til en sikker adfærd.



Figur 3.12: Fertig m.fl. (2020) awareness modenhedsmodel

Som beskrevet i afsnit 2.3, deler Fertig m.fl. (2020) Awareness modenhed op i fire forskellige områder. Disse områder kan påvirkes enkeltvis for at øge awareness modenheden og på den måde ændre adfærden hos brugerne. I dette afsnit vil de fire områder undersøges enkeltvis i forhold til awareness modenhed i Hjørring Kommune.

Knowledge and Skills

En af de første ting projektets interviewpersoner bliver spurgt ind til er deres bevidsthed omkring CSA. Dette er også, hvad der bliver kaldt knowledge and skills i modenhedsmodellen. Her bliver der som tidligere beskrevet ikke vurderet på den enkelte interviewpersons tekniske evner, men i højere grad deres evner til at anvende deres viden om CSA i praksis. Det, der er interessant at observere ved dette, er, at der forud for spørgsmålet ikke bliver tilkendegivet, hvilken slags cybersecurity der omtales.

Sammenligner vi hvordan de forskellige interviewpersoner besvarer spørgsmålet, bliver det hurtigt tydeliggjort at der er forskellige opfattelser af CSA.

> *"Jeg tror, jeg er mere bevidst om, hvilke søgemaskiner jeg bruger, når jeg browser på nettet. Jeg er bevidst om, hvilke apps jeg giver tilladelse til, på min telefon for eksempel. Jeg er bevidst om, hvad jeg siger, hvornår, i forhold til, om der er nogen ting, der optager det, jeg siger. I forhold til algoritmer og sådan nogle ting."*
> (Skolelærer - Bilag 1, 04:15 [1.5])

Her beskriver skolelæreren, at han opfatter CSA som værende en sikker måde at manøvre sig rundt på internettet, med fokus på hvilke tilladelser tjenester på internettet kræver. Kigger vi i stedet på

en afdelingsleder på handicapområdet, bliver CSA primært forbundet med GDPR-lovgivningen, og de udfordringer det kan skabe i det daglige arbejde på det sociale tilbud.

> *". . . Og så er det også det her med, at så må vi ikke gemme alle navnene i den samme sag. Det er vel en del af journaliseringsdelen, det kan godt være, jeg blander det en lille smule sammen. Når vi laver lister med CPR-numre som vi skal bruge til noget aftjekning så må de ikke ligge sammen og altså, alt det der, som kan komme til at fylde i hverdagen, hvor det ville være nemt, hvis man bare lige kunne... men det kan man så ikke"*
> (Afdelingsleder, Handicapområdet - Bilag 2, 02:01 [2.1])

Skolelæreren udtaler også, at han tror, det ville være en god idé at bruge CSA mere i daglig tale, så det kan blive en mere integreret del af deres hverdag. Han nævner, at begrebet godt kan have mange forskellige opfattelser. Det er derfor vigtigt for ham, at der bliver informeret omkring det.

> *"Det tror jeg, det er kun bare det her med at få det afmystificeret på en eller anden måde. Sådan at alle, mere eller mindre, ved, hvad det handler om. Det tror jeg, jeg ville gøre meget ved, at det var noget, man også kom til at snakke om. Og noget, der var mere fokus på hos alle medarbejdere. Og dem, som har en idé om, hvad det handler om"*
> (Skolelærer - Bilag 1, 08:12 [1.9])

Når medarbejdere mangler viden, er der større risiko for at de bryder IT-politikker, da de ikke er blevet oplyst omkring dem. I dette eksempel er det demenskonsulenten, som ikke har fået træning i, hvordan oprettelsen af passwords fungerer. Demenskonsulenten arbejder på tværs af mange institutioner, og har derfor mange passwords gemt, som hun har behov for på daglig basis. Det kan derfor blive svært for hende at huske dem alle. Af den grund har hun nedskrevet sine passwords på en seddel, hvilket hun først fik oplyst var imod IT-politikken, da hun var ved IT-afdelingen grundet et teknisk problem.

> *"Men vi bliver ikke oplært i det. Det var jo helt tilfældeligt det der. Jeg tror faktisk, det var fordi, der var et eller andet, jeg var inde her ved IT. Og så, hov, du har altså gemt din kode, det må du jo ikke. Nå, men så skal jeg jo sidde og huske det hver eneste gang, og når man så skifter sig i det måde, hvad man var nu lige, det var altså noget ikke. Så er det meget lettere, at den lige er gemt. Og det må du altså ikke. Nå, okay. Det var jeg jo ikke klar over"*
> (Demenskonsulent - Bilag 3, 15:49 [3.11])

Der er altså en forskellighed i modenheden indenfor viden og anvendelse af denne viden i forhold til CSA. Det viser sig, at en lavere modenhed kan føre til overtrædelse af interne politikker, men også til forskellige forståelser af CSA generelt. I snakken med demenskonsulenten blev det også klart, at vedkommende faktisk tænkte over CSA i hverdagen, men ikke var klar over de interne politikker eller, at der fandtes et begreb for det. Dette kan være et tegn på, at dette område omkring 'Knowledge and skills' kan være en fordel at have fokus på i forhold til at ændre adfærden - eksempelvis som ved demenskonsulenten - til en mere sikker adfærd.

Salience

Salience skal i denne forbindelse forstås som, hvorvidt medarbejderne tænker over CSA i deres hverdag. Dette er en betydelig faktor, da det giver indsigt i hvorvidt medarbejderens viden er fremtræden i deres hverdag, eller om deres viden er mere bagvedliggende. Fertig m.fl. (2020) model i figur 3.12 foreskriver, at jo mere en medarbejder aktivt tænker over deres adfærd i forbindelse med CSA, jo større er chancen for at deres adfærd så også er sikker eller compliant med organisationens sikkerhedspolitikker.
Flere respondenter erkender, at CSA ikke er fremtræden i deres tanker i deres dagligdag.

> *"I hverdagen tænker jeg ikke ret meget over det. Jo, på helt lavpraktisk niveau, tænker jeg over det"* (Afdelingsleder, Handicapområdet - Bilag 2, 08:29 [2.7])

Dette er dog ikke det eneste eksempel på, at CSA ikke er fremtræden i hverdagen hos medarbejdere. Således fortæller en skolelærer også følgende:

> "Det fylder jo ikke meget. Det er nok mere i min underbevidsthed, tror jeg .Jeg tror ikke, jeg synes, det skal fylde mere for mig"(Skolelærer - Bilag 1, 07:01 [1.7])

Det er dog ikke alle respondenterne, der giver udtryk for, at CSA ikke er fremtræden i deres tanker i hverdagen. Således giver en bibliotekar udtryk for, at CSA fylder en del i hverdagen:

> *"Det er top vigtigt synes jeg, ja, helt sikkert, men også fordi vi er sådan et, måske i forhold til andre organisationer, så biblioteket er bare gennemdigitaliseret, altså meget af det vi laver, alle transaktioner, vi har engang imellem, hvor vores biblioteksystem går ned, ikke hacket, men der er nedetid, og når der er det, så går organisationen mere eller mindre i stå, altså man kan godt finde nogle bøger frem manuelt, men du kan ikke låne dem ud, du kan ingenting. Det er bare så meget vores organisation og være digital og der kunne jeg forestille mig at det kunne gå knap så galt hvis man er i en børnehave eller et eller andet i den stil, så ja, det fylder."*
> (Bibliotekar - Bilag 4, 25:18 [4.21])

De foregående citater viser altså, at der hovedsageligt ikke tænkes bevidst over CSA i hverdagen hos de fleste medarbejdere i Hjørring Kommune. Der er dog undtagelser, som eksempelvis bibliotekaren fra forrige citat. Det kan dog tænkes, at lige netop biblioteker har stort fokus på lige netop CSA, da der har været tidligere udfordringer på biblioteker med cybersecurity - blandt andet keylogging.
Disse skrækhistorier fra omverdenen fungerer således som motivation for, at CSA er fremtræden i hverdagen.

> *"...men noget som også gøder det er jo for eksempel sådan noget som nyheder, når man så ser at alt muligt bare bliver hacket fra en side af, eller at der har været brud på et eller andet, det ville jeg så også våge at påstå at er med til det implicit. At folk kommer i tanker om, som jeg også nævnte før at verden er bare mere usikker end man måske tror"*
> (Bibliotekar - Bilag 4, 24:41 [4.20])

Der kan argumenteres for at graden hvori CSA er fremtrædent i interviewpersonernes arbejdsgang, er afhængigt af deres stilling, samt den del af organisationen de arbejder i. Det vil naturligt forekomme, at CSA er betydeligt mere fremtrædent for medarbejderne i databeskyttelse, som til dagligt arbejder med CSA. Formålet med frameworket i denne rapport er dog at flytte CSA fra et individuelt perspektiv til at omfavne hele organisationen. Derfor bliver man nødt til at opfatte organisationen som en helhed i forhold til deres awareness modenhed - hvilket så også er tilfældet med 'Salience'. Det virker derfor til, ud fra empirien, at der er en generel tendens til, at CSA har en lavere fremtræden hos medarbejdere i Hjørring Kommune. Dette kan derfor være et relevant punkt at arbejde med, for at sikre en mere sikker og compliant adfærd.

Intention

Det kan være relevant at undersøge intentionen hos interviewpersonerne i Hjørring Kommune. Dette giver indblik i hvor vigtigt de mener, CSA er for deres respektive afdeling eller stilling. Deres opfattelse af vigtigheden af CSA er brugbart til undersøgelsen af Hjørring Kommunes awareness modenhed, da medarbejdernes lyst til CSA kan være en afspejling af organisationens samlede holdning. Denne tanke kommer ud af, at hvis organisationen ikke får formidlet vigtigheden af CSA korrekt, vil den heller ikke komme til syne hos den enkelte medarbejder. Følgende citat kan være et eksempel på, at dette ikke er tilfældet:

> *"Det tror jeg, det er kun bare det her med at få det afmystificeret på en eller anden måde. Sådan at alle, mere eller mindre, ved, hvad det handler om. Det tror jeg, jeg ville gøre meget ved, at det var noget, man også kom til at snakke om. Og noget, der var mere fokus på hos alle medarbejdere. Og dem, som har en idé om, hvad det handler om."*
> (Skolelærer - Bilag 1, 08:12 [1.9])

Generelt virker det dog til, at der er en intention hos de interviewede medarbejdere i Hjørring Kommune omkring at udvise en sikker adfærd. Intentionen om at have håndhæve en sund CSA kultur i organisationen kan også komme fra et personligt ønske om ansvar overfor de borgere som man servicerer. I den nedenstående citat fra bibliotekaren giver han udtryk for at han ønsker at biblioteket skal være et sikkert sted for borgerne at komme, og at han derfor ønsker at opretholde sikkerheden på hans arbejdsplads.

> *"...når man arbejder med nogle systemer, hvor man så har, det er sådan respekt overfor dem som bruger biblioteket på en eller anden måde, at man ligesom opfører sig ordentligt, passer på deres ting ik'. Det ville være det samme hvis jeg var en mekaniker og nogen kom og afleverede deres bil, så passer jeg også på den, altså på den måde ikke. At man sådan ligesom, jeg tror det er det, at man sådan er et ordentligt mennesker, hvis man skal op på en eller anden etisk platform, men ja, det kan man jo også sagtens være uden at være aware kan jeg godt se, men ja, jeg tror det er det, et eller andet sted, at der er en respekt for det man laver..."*
> (Bibliotekar - Bilag 4, 21:25 [4.18])

> *"...Altså der er ikke noget som er sikkert, sådan længere på en eller anden måde. Så derfor får man også lyst til måske at sikre sig så godt som man kan..."*
> (Bibliotekar - Bilag 4, 12:00 [4.9])

Afdelingslederen i handicapområdet giver udtryk for at hun har en intention at om hendes medarbejdere kan opretholde sund CSA kultur, men da hun godt selv kan støde ind i udfordringer med forståelsen, eller manglen på værktøjer, kan det være svært for hende at formidle videre. Her er intentionen god, men empirien viser at intentionen ikke kan stå alene, og der er en nødvendighed for supporterende værktøjer.

> *"Så jeg synes, det er vigtigt, men det bliver også lidt tungt. Så for mig er det både det ene og det andet."*
> (Afdelingsleder, Handicapområdet - Bilag 2, 02:01 [2.4])

Som det ses i ovenstående citater, er der en konsensus omkring vigtigheden af CSA og en intention om at udvise en sikker adfærd i hverdagen. Dog vises der også en tilbageholdenhed, fordi CSA "bliver lidt tungt". Det virker altså som om, der er en intention og en forståelse for, at det er vigtigt, men alligevel en eller anden barriere, der holder medarbejdere tilbage i forhold til at ændre adfærd. Som det blev vist tidligere i afsnit 3.1, deler medarbejdere i kommunen en forståelse af, at det er IT-afdelingens ansvar at stå for CSA i organisationen. Det kan tænkes, at blandt andet denne forståelse kan være en af de barrierer, der kommer til syne her. IT-afdelingen i Hjørring Kommune arbejder dog målrettet mod at udbrede CSA på tværs af organisationen, hvorfor det er fordelagtigt, at medarbejderne udviser en intention om at ville være en del af dette. Dette behov for udefrakommende indgriben, kan eksempelvis ses i følgende citat:

> *"...men det med at få belyst det på en eller anden måde. At der er nogen, der kommer og fortæller om det. Sætter fokus på det på en anden måde måske. Det tror jeg godt, man kunne nå langt med"* (Skolelærer - Bilag 1, 08:42 [1.10]

Habit

For at få indsigt i Hjørring Kommunes indsats med CSA, er det også essentielt at fokusere på, hvordan interviewpersonerne begår sig med cybersecurity i deres daglige arbejdsgang i form af vaner. Adfærd er i høj grad præget af vaner, og vaner er en stor del af en hverdag. Dette område vil derfor undersøge respondenternes vaner i forhold til CSA.

> *"...Ugh, jeg er begyndt at afvise cookies, fordi jeg tænker sådan, det skal man nok. Man gør det sådan lidt hovedløst, indtil jeg fandt ud af, jeg får det samme ind på mine medier. Men jeg gør det lidt hovedløst. Desværre"*
> (Afdelingsleder, Handicapområdet - Bilag 2, 08:29 [2.7])

En afdelingsleder på handicapområdet udtaler, at CSA ikke er noget de beskæftiger sig meget med i hverdagen. Som et tilbud til førtidspensionister, der beskæftiger sig med produktion er de i sin natur meget analoge i deres arbejdsgange, det er derfor kun det fastansatte personale der anvender computere. Vanerne i hverdagen i forhold til CSA, bliver i stedet på et niveau af "det skal man nok", som det ses i citatet ovenfor, og ikke bevidste handlinger.

Dette kunne tyde på en lavere awareness modenhed i forhold til de daglige vaner. Dette kan eksempelvis også ses i prioriteringen af CSA i forhold til andre daglige opgaver.

> *"Har jeg egentlig forståelse, eller har jeg viden omkring det? Nej, det har jeg måske nok ikke. Så bliver det nedprioriteret på en eller anden måde. I forhold til de andre ting, der foregår i løbet af sådan en hverdag."*
> (Skolelærer - Bilag 1, 06:21 [1.6])

Skolelæreren giver udtryk for, at manglende viden eller oplysning omkring CSA, fører til nedprioritering i hverdagen. Det kunne derfor indikere, at medarbejdernes vaner er at nedprioritere CSA, fordi de ikke har tilstrækkelig forståelse for begrebet. Omvendt kan der argumenteres for, at oplysning til medarbejderne er en forholdsvis simpel løsning for organisationen, for at ændre medarbejdernes adfærd.

At ændre vaner er dog alligevel ikke så simpelt. Flere af respondenterne nævner, at der flere gange har været fokus på at låse sin pc når man går fra den. Dette er der dog mange, der ikke gør, selvom der er fokus på det fra IT-afdelingen.

> "Helt lavpraktisk, så har vi jo et biblioteksrum, altså vi har låste døre ind til vores kontorer og sådan noget, det skal man have og vi skal låse vores computere når vi går fra dem, det skal man, det siger Ulla som sidder lige herude. Men det giver også god mening fordi de står åbne med adgang direkte ind til kommunens IT infrastruktur, så hvis man får fat i en af vores computere, og ved hvad man laver, så har man altså adgang til en del. Men sådan noget som det at lige at trykke lås når man går, den er svær. Allerede der bliver det svært. Så kan man sige, det er spændet på awareness-delen, den viser det faktisk meget godt, at der er nogen, jeg er sådan lidt fascistoid omkring det og låser også andres computere, hvis jeg lige kommer forbi en, så siger jeg lige "plup"og så, men der er også andre som tænker, årh det går nok, jeg skal bare lige herover"(Bibliotekar - Bilag 4, 32:21 [4.27])

Dette er et eksempel på, at en forholdsvis simpel ting som at låse sin computer når man går fra den, kan være svært at gøre til en vane, hvis det ikke allerede er. Det virker altså til, at der findes en del indbyggede vaner blandt medarbejdere i Hjørring Kommune, som kan være en udfordring at ændre på i forhold til CSA.

> *"Nej jeg tror faktisk lige netop ikke, det kan godt være det er paradoksalt i forhold til mange andre steder, men jeg synes ikke vi har været ude i noget med at det er blevet egentligt mere besværligt, men det er bare sådan noget med at man skal gå fra sådan noget "vi plejer" til nårh nu skal du lige gøre det på den her måde, fordi om jeg skal finde dit CPR nummer inde i vores bibliotekregister eller om jeg skal finde dit lånernummer som det så hedder, sådan et randomt genereret nummer det er samme forskel arbejdsmæssigt, men det er det bare ikke for din datasikkerhed kan man sige*
> (Bibliotekar - Bilag 4, 10:45 [4.8])

Foregående citat viser et eksempel på, hvordan der kan arbejdes med vaner. Her giver en bibliotekar et eksempel på, at hvis man kender til arbejdsprocesserne og de daglige vaner i forvejen, kan der arbejdes med disse på en måde, der tager hånd om dem. Dette kunne eksempelvis være, ikke at ændre i selve vanen eller processen, men i stedet ændre eksempelvis CPR-nummeret til et generisk lånernummer, der så sikrer en sikker adfærd.

Baseret på dette afsnit omkring Hjørring Kommunes awareness modenhed indenfor 'habits', virker det til, at de daglige vaner for respondenterne ikke er særlig modne i forhold til CSA.

Det bliver ofte nedprioriteret i hverdagen, dels fordi der mangler forståelse for begrebet, men også fordi de daglige kerneopgaver opfattes som langt vigtigere. Yderligere, viser analysen, at det kan være vanskeligt at ændre vaner såsom at huske at låse sin pc når man forlader den. Der ses dog også muligheder for at identificere disse vaner og på den måde starte arbejdet med dem.

Environmental Constraints

Et af de punkter i modenhedsmodellen, se figur 3.12, som Hjørring Kommune kan have direkte indflydelse på er Environmental Constraints. Fertig m.fl. (2020) beskriver dette punkt i modellen som de barrierer, der står i vejen for medarbejdernes adfærdsændring, når det kommer til CSA. Environmental Constraints kan dog også forekomme i form af eksempelvis lovgivning og regulativer, hvor Hjørring Kommune så ikke kan have direkte indflydelse. Vi har valgt at fokusere på de Environmental Constraints som Hjørring Kommune kan have indflydelse på, da det ikke er muligt at ændre eksempelvis lovgivning. Det er dog stadig relevant at have in mente, at dette også kan have indflydelse på den sikre adfærd.

En begrænsning, der går igen igennem de foretagede interviews, er mangel på tid i hverdagen. De daglige kerneopgaver fylder så meget i hverdagen, at der simpelthen ikke er tid til at fokusere på CSA. En skolelærer mener eksempelvis, at det kan være udfordrende for lærerne at finde tid til at enten opsøge information om CSA selv, eller gennemgå træninger. Tiden er knap i deres fag, så det er sjældent de har tiden til at have fokus på CSA.

> *"Det er et rigtig svært spørgsmål. Også fordi, at der er mange, som i det her fag synes tiden er knap. Og det der med at få de rigtige ting ind. Også specielt, når det er noget, der måske skal foregå ud over den hele arbejdstid. Så er det faktisk rigtig, rigtig svært at finde ud af, hvordan og hvor ledes kan man det. Men det kunne da sagtens være... Altså det der med bare lige at sidde med et program, den ved jeg ikke. Men det med at få belyst det på en eller anden måde. At der er nogen, der kommer og fortæller om det. Sætter fokus på det på en anden måde måske. Det tror jeg godt, man kunne nå langt med"*
> (Skolelæreren - Bilag 1, 08:42 [1.10])

Skolelæren pointerer yderligere, at grundet deres minimale tilgængelige tid til “ekstra” arbejdsopgaver, er det specielt vigtigt at opgaverne har en mening. Der skal være et ordentligt belæg for at de skal tage timer ud af deres pressede arbejdsskema, for at deltage i CSA træninger.

> *"Jeg tror i hvert fald lige med lærer, sikkert med rigtig mange andre mennesker også. Det skal give mening. Der skal være en idé med, at vi sidder over to timer på at høre om cyber security eller hvad nu"*
> (Skolelærer - Bilag 1, 11:53 [1.13])

En anden begrænsning som kommer til syne blandt respondenterne, er manglende materiale til oplysning eller oplæring af medarbejdere i CSA. En af udfordringerne som afdelingslederen for handicapområdet møder i hendes arbejde med et socialt tilbud for borgere, er at hun føler hun godt kan mangle værktøjer til at videreformidle CSA til hendes ansatte, som primært er ældre, ofte med lavere kendskab til IT.

> *"Nej, men jeg synes, det giver noget pangel. Det bliver sådan lidt tungt, nogen gange. Men det er fordi, jeg forstår godt, hvorfor vi skal bruge det. Når jeg så skal videreformidle til min personalegruppe, hovedsageligt håndværkere over 50. Når jeg skal formidle de her ting så bliver det lidt tungt"*
> (Afdelingsleder, Handicapområdet - Bilag 2, 13:21 [2.9])

Denne udfordring kommer også til syne i databeskyttelsesteamet, der ligeledes ikke har færdiglavede og testede værktøjer til rådighed til at oplyse og oplære omkring CSA. I stedet må de selv bygge disse værktøjer. En årsag til at disse værktøjer ikke findes, kan være, at CSA som begreb stadig er meget nyt, hvorfor der ikke er forsket nok i det endnu til at dette materiale eksisterer.

Trods denne udfordring har afdelingslederen forsøgt sig med at bryde informationen ned i mindre og mere overkommelige formater. Hendes erfaringer viser at dette kan være en bedre måde at formidle information til denne målgruppe, da informationen er kort, og tilgængelig i de specifikke scenarier hvor de ansatte har behov for information.

> *"Nej, jeg giver dem de små tips. Jeg gør det nemt, i skal huske det, det og det, så jeg tager dem i små punkter ud fra, hvad jeg piller ud, hvad de skal være opmærksomme på"*
> (Afdelingsleder, Handicapområdet - Bilag 2, 13:57 [2.10])

Tager man udgangspunkt i teorien fra Fertig m.fl. (2020), giver det mulighed for at inddele Hjørring Kommune i én af tre modenheds niveauer. Som tidligere beskrevet er disse niveau fordelt i *perception*, *protection* og *behavior*, hvor behavior er det højeste modenhedsniveau.

Vi kan fra empirien udlede, at størstedelen af interviewpersonerne giver et indtryk for at Hjørring Kommunes awareness modenhedsniveau ligger mellem perception og protection. Denne vurdering er udarbejdet på baggrund af deres evne til at forstå, hvordan mulige sikkerhedsbrister identificeres, samt en delvis evne til at beskytte sig imod disse.

IT-afdelingen indeholder et databeskyttelsesteam, der arbejder strategisk med beskyttelsen af data, der håndteres i kommunen. Dette gælder også arbejdet med CSA. Dette er et argument for, at Hjørring Kommune ikke er i niveau 1 i Fertig m.fl. (2020) modenhedsmodel. Kommunens investering i IT-afdelingens databeskyttelsesteam viser et fokus og en udvikling i forståelsen af vigtigheden af CSA. En medarbejder i databeskyttelsesteamet forklarer det således:

> *"Altså, nu ved de godt, hvad en phishing-mail er. De ved, hvad det er, og de ved, hvad man skal og ikke skal gøre. Nu er de nået over begynderniveauet. Nu skal vi lige have dem på mellemniveau. Og det er det, vi springer i gang med at tage."*
> (Medarbejder i databeskyttelsesteamet - Bilag 5, 05:27 [5.4])

En yderligere opsamling på Hjørring Kommunes modenhedsniveau i forhold til CSA vil præsenteres i følgende afsnit.

3.4 Opsamling af analysen

Analysen af forståelsesrammerne omkring CSA fandt tre områder, hvor der opstår inkongruens mellem de to grupper. Dette sker i forståelsen af, hvad CSA er, i forståelsen af, hvorfor CSA er nødvendigt og i forståelsen af, hvordan CSA kommer til syne i hverdagen.

Forståelsen af, hvad CSA er, er en anelse forskellige mellem de to grupper. Medarbejdere i databeskyttelsesteamet har en forståelse af, at CSA ansvar for databeskyttelse. Denne databeskyttelse skal ske ved at udbrede CSA på tværs af organisationen. Medarbejdere i andre kommunale stillinger har en forståelse af, at CSA er en forebyggende indsats, der ofte opleves som en hindring i deres hverdag i forhold til deres kerneopgaver. Yderligere, ser denne gruppe CSA som et ansvar for IT-afdelingen.

Forståelsen af, hvorfor CSA er nødvendigt viser ligeledes en forskellighed blandt de to grupper. Medarbejdere i databeskyttelsesteamet har en forståelse af, at CSA er nødvendigt, fordi data snart er en del af samtlige stillinger i en moderne organisation, hvorfor det er nødvendigt at alle føler et CSA ansvar. Medarbejdere i andre kommunale stillinger har en forståelse af, af CSA er vigtigt, men mangler forståelse for, at det er ligeså vigtigt som deres kerneopgaver.

CSA kommer ligeledes til syne på forskellige måder i hverdagen for de to grupper. Medarbejdere i databeskyttelse forstår CSA som et strategisk værktøj til databeskyttelse, hvor medarbejdere i andre kommunale stillinger har en forståelse af begrebet på baggrund af deres hverdag, hvor CSA kommer til syne. Dette skaber ligeledes inkongruens blandt forståelserne.

Hovedpointerne i de teknologiske forståelsesrammer, er altså en inkongruens i forståelsen af, hvem der har ansvaret for CSA, hvor meget CSA skal fylde i hverdagen og, hvordan forståelsen af, hvorvidt CSA er en del af deres kerneopgaver i de forskellige stillinger.
Ser man disse hovedpointer i forhold til analysen af kulturen i forhold til CSA, ses det, at nogle af disse hovedpointer går igen i domæneanalysen.

Domæneanalysen fandt frem til tre hovedpointer i forhold til kulturen omkring CSA i Hjørring Kommune; ansvaret omkring CSA, udbredelsen af CSA og adfærden angående CSA.

Forståelsen af ansvaret og ansvarsbevidstheden hos interviewpersonerne udenfor databeskyttelsesteamet er i bred enighed om, at hovedansvaret af CSA ligger hos IT-afdelingen og databeskyttelsesteamet, men anerkender samtidig vigtigheden af CSA.

Databeskyttelsesteamet arbejder omvendt på at udbrede CSA i organisationen, fordi ansvaret bør være delt, da medarbejdere i alle stillinger arbejder med data.
Strategien fra databeskyttelsesteamet for udbredelsen af CSA i kommunen, har en stor betydning og er en succesfaktor når det kommer til det nuværende niveau som er fundet af CSA i Hjørring Kommune. Strategien lyder på at have fokus på åbenhed, afmystificering gennem humor, fysisk fremmøde og i den forbindelse dialog og kommunikation med medarbejdere indenfor forskellige organisatoriske områder i organisationen.

Denne strategi har til formål at ændre adfærden hos medarbejdere i kommunen til en mere sikker og compliant adfærd. Dog ses det, at kulturen kan spænde ben, da adfærden på nuværende tidspunkt strider lidt imod denne ændring.
Flere medarbejdere anser CSA som en hindring og nedprioriterer det i deres hverdag.
Den sprogmæssige udfordring som Hjørring Kommune oplever kommer gennem at CSA er et sjældent emne der bliver diskuterret i diverse organisationsled og områder, hvorpå CSA får et element

af mystik tilføjet udover de tilfælde, hvor databeskyttelsesteamet kommunikerer med medarbejderne.

Analysen af kulturen viser altså, at denne lader til at have indflydelse på forståelsesrammerne. Ligesom det ses i forståelsesrammerne, lader kulturen og opbygningen af organisationen til at lægge ansvaret for al IT hos IT-afdelingen.
Dette virker som det mest fornuftige, da organisationens IT-eksperter arbejder i IT-afdelingen, ligesom økonomi-eksperter arbejder i økonomi-afdelingen og så fremdeles.
Dog kan der argumenteres for, at CSA ikke blot er en opgave for en IT-afdeling i takt med digitalisering i alle arbejdsroller. Dette betyder, at denne kultur omkring en skarp opdeling af ekspertiseområder modvirker forsøget på at forankre CSA i organisationen.
Analysen viser, at der arbejdes på at ændre denne kultur i Hjørring Kommune i forbindelse med arbejdet med forankringen af CSA. Her anvendes især humor, åbenhed og dialog til at udbrede forståelsen og kendskabet til CSA. Det virker til, at dette vil virke, da empirien viser, at dette er, hvad medarbejdere i andre kommunale stillinger efterspørger.
Denne åbenhed og dialog tyder ligeledes til at være den rette metode til i sidste ende at ændre adfærden hos medarbejderne. Hvis inkongruensen i forståelsesrammerne i form af forståelsen omkring ansvar, hvor meget CSA skal fylde i hverdagen og, hvorvidt det er en kerneopgave for alle, kan ændres til fælles forståelse gennem dialog, kan denne adfærd potentielt følge med.

Analysen af Hjørring Kommunes awareness modenhed viser, at medarbejdernes vidensniveau omkring CSA kan være meget forskellige. Flere af medarbejderne mener, at de godt kunne bruge noget træning og oplysning i cybersecurity. Yderligere udviser de også et ønske om, at konceptet bliver mere italesat i hverdagen, hvilket er paradoksalt, da de samtidig ikke mener, det skal fylde mere.
Dog viser analysen også, at det ikke er alle medarbejderne, der aktivt tænker over CSA i deres hverdag. Deres tanker omkring CSA viser sig oftest når der emnet bliver omtalt udefra, f.eks. når de hører om sikkerhedsbrud i samfundet. I analysen findes der også, at medarbejderne har gode intentioner vedrørende CSA. De ønsker at håndhæve en sund CSA kultur i deres organisation. De gode intentioner kan i nogle tilfælde spores tilbage til et ønske om at yde en god service for borgerne i kommunen, samt ønsket om at skabe et sikkert sted at færdes digitalt.
Et af hovedpunkterne i denne analysedel er at identificere hvilke *environmental contraints* der kan forekomme i organisationen. Dette er barrierere der kan stå i vejen for at medarbejde kan opnå den ønskede CSA kultur. Her findes det at det kan være svært for medarbejderne at finde tid i deres allerede tidpressede arbejdsdag til at dygtiggøre sig i CSA. Det vises også i analysen at trods et ønske om bedre CSA kultur, kan det være svært at videreformidle i organisationen, hvis de rigtige værktøjer er svært tilgængelige. Slutteligt i denne analysedel bliver der vurderet at Hjørring Kommunes awareness modenhedsniveau kan ligge mellem niveauerne *perception* og *protection*.

Empirien lader i hvert fald til at vise, at kulturen i forholdsvis høj grad lægger fundament til at skabe en fælles forståelsesramme, eller i hvert fald større fælles forståelse. En god start er i hvert fald at anderkende disse forskellige forståelser, hvilket er tilfældet i Hjørring Kommune.

4 | Diskussion

Dette afsnit vil indeholde en diskussion omkring centrale emner i rapporten. Igennem rapporten har ansvar været et centralt emne, hvorfor dette vil blive diskuteret fra forskellige perspektiver. Herefter vil følge en diskussion omkring udvidede forståelsesrammer, baseret på andet teori. Til sidst vil følge en diskussion omkring kulturelle analyser i forhold til den teknologiske forståelsesrammestruktur for denne rapport.

4.1 Hvem har ansvaret for CSA?

Gennem arbejdet med denne rapport, var der et gennemgående tema, som gik igen blandt interviewpersonerne, hvilket ikke var forventet, da scopet for dette projekt blev lavet, nemlig hvem der har ansvaret for CSA på samfundsmæssigt niveau.

Ansvar er et tema, der går igen igennem arbejdet med CSA. Vores litteraturstudie, der blev udarbejdet før dette speciale, fandt ligeledes ansvar som et koncept, der går igen i litteraturen. Her var der dog fokus på ansvaret internt i organisationen - hvorvidt det var IT-afdelingens ansvar eller, hvorvidt den enkelte medarbejder også havde et ansvar.
Igennem arbejdet med denne rapport er der dog kommet andre interessante syn på ansvarskonceptet fra interviewpersonerne. Her blev ansvaret diskuteret på tre niveauer; individuelt, organisatorisk og samfundsmæssigt.

Individuelt ansvar

Der var bred enighed blandt interviewpersonerne om, at når samfunds- og arbejdsopgaver bliver mere og mere digitaliserede, så er den individuelles CSA forståelse et emne som skal bringes op i dialog. Som dansker, kan det argumenteres for, at en persons CPR-nummer er noget af det mest personlige data som kan udgives, da det er den talrække som gør de forskellige individers digitale fingeraftryk i systemernes database, hvor alt dataen om personen er forbundet til det nummer. Danmark er et meget digitaliseret land, hvorfor den individuelles ansvar for at passe på ens personlige oplysninger og digitale fingeraftryk er et mere fremtrædende problem end det kan være i andre samfund.

Der kan fremstilles en interessant kontrast når det kommer til individets personlige ansvar. De fleste danskere forstår vigtigheden af at holde deres persondata tæt, når det direkte påvirker dem selv. Trods dette er det fortsat en stor udfordring at overbevise medarbejdere i organisationer om at passe på data som virksomheden håndterer, selvom det i sidste ende også kan være et personligt ansvar.

Denne stadig større og bredere digitalisering, rejser spørgsmålet om, hvor meget ansvar hver enkelt har for at kende til og udvise en sikker adfærd på arbejdspladsen. Der kan argumenteres for, at den enkelte har noget ansvar, da arbejdet netop i stadig højere grad foregår digitalt - i alle stillinger i moderne organisationer.

Organisatorisk ansvar

I forbindelse med implementeringen af GDPR lovgivningen i EU, er vigtigheden af persondata, seriøsiteten ved håndteringen og opbevaringen blevet anerkendt, i hvert fald på virksomhedsniveau. Som beskrevet før, er private personer tilbøjelige til at skrive deres CPR-nummer ofte, hvilket kan vise en uforsigtighed på det individuelle plan. Dog er det blevet vist i denne rapport, at Hjørring Kommune har kunne omgå dette på et organisatorisk niveau, ved eksempelvis at tildele borgere et lånernummer på biblioteket frem for CPR-nummer.

Det initiativ som er vist gennem GDPR er ikke sket direkte i forbindelse med cybersecurity og cybersecurity awareness, men derimod mere som et persondatahåndteringsregulativ. CSA og persondata før GDPR er sammenligneligt på baggrund af at begge koncepter omhandler noget ikke-kvantificerbart materiale, som er uhåndgribelig af natur, grundet manglende viden omkring emnet på et samfundsmæssigt og et individuelt plan.

Denne mangelende forståelse af CSA som koncept har skabt en dualitet, hvor der er en bred enighed mellem interviewpersonerne, at verden bliver mere og mere digitaliseret, hvilket betyder, at der naturligt bliver brugt mere tid foran en skærm. Denne dualitet opstår, hvor personer bruger mere tid foran teknologi, men ikke har en forståelse for eller en stærk ansvarsfølelse om, at sikkerhed er en naturlig proces indenfor den øgede brug af teknologi. Når sikkerheden ikke går hånd i hånd med brugen af IT, skaber det en mismatch i forbindelse med kerne forståelsen af, hvorfor teknologien bliver anvendt og hvad dens rolle er i hverdagen. Flere interviewpersoner nævner, at en potentiel årsag kan være, at de ældre generationer ikke har fået kapabiliteterne eller know-how'en til at følge den teknologiske udvikling mod de generationer som er opvokset med det.

Årsagen til dette kan være, at ældre generationer har set det som værktøjer, der kan tilvælges, hvor de nyere generationer ikke har haft det valg, hvilket har tvunget dem til at være afhængige af teknologien, da det er der den største trafik i forbindelse med information, underholdning og lignende foregår. Den ældre generation har haft valget om at være aktive forbrugere, og hvilket forhold de har til teknologien som forbrugere, hvor de nyere generationer ikke har haft samme valg. Dette kan have skabt den førnævnte mismatch i forståelse og brug af de teknologiske muligheder som er forekommet. Dette pårører også, hvorfor det kan være svært at indføre ændringer i medarbejderes handlinger, influere deres forståelse og organisationens kultur, som blev uddybet i 3.1 og 3.2.1 i analysen.

Samfundsmæssigt ansvar

Dette element af overbevisning er fremherskende på grund af den førnævnte dualitet. I forbindelse med, at de nyere generationer har det nødvendige forhold til IT, er der bred enighed fra interviewpersonerne, at der er et samfundsmæssigt ansvar til at få et kendskab til CSA, som burde starte allerede i folkeskolen.

Udover de yngre generationer, er der også en udfordring til, hvordan man får en bedre forståelse på tværs af de ældre generationer, hvor løsningen er fundet, gennem litteraturstudiet, til at lave specifikke træninger i forbindelse med det område folk arbejder indenfor, mindsket stress og gøre det til mere end bare et e-læringsværktøj (Hoeing m.fl., 2022). Selvom den lavpraktiske tilgang kan være effektiv hos Hjørring Kommune, er det ikke nødvendigvis tilfældet, når det kommer til andre organisationer, kommuner eller områder i markedet.

Effektiviteten ved implementeringen af GDPR stiller spørgsmål til, om hvorvidt CSA på samfundsniveau burde udføres lovgivningsmæssigt af staten eller EU, eller hvorvidt markedet selv har ansvaret for det. Der kan argumenteres for at den optimale måde at implementere CSA på samfundsniveau burde være lovgivningsmæssigt, som der blev gjort med GDPR-lovgivningen, da markedet ikke har det nødvendige incitament til at gennemtvinge en sådan implementering.

I forbindelse med det tidligere nævnte mismatch, kan den manglende kvantificerbarhed af CSA eller forståelsen af CSA gøre, at vigtigheden ikke kommer til syne hos aktørerne i de forskellige ansvarsniveauer. Det kan altså tænkes, at der mangler en generel ansvarsfølelse blandt disse niveauer, eller blot en forventningsafstemning omkring, hvem der skal have dette ansvar. Dette kan netop skyldes denne manglende kvantificerbarhed af CSA eller, at det er så nyt et emne, at der mangler viden omkring det stadig.

Et andet fænomen indenfor CSA, som ikke ofte er påtalt, er, at niveauet af indsatsen af CSA i virksomheder ikke skal overgå den økonomiske værdi som deres intellectual property, (IP) rettigheder, er værd. Hvis det skulle reguleres fra et lovgivningsmæssigt perspektiv, hvordan beslutter man så, hvilke industrier disse lovgivninger skal være indenfor. Som nævnt i introduktionen er angreb fra ondsindede aktører mere relevant nu end nogensinde før, men har CSA stor nok værdi til at virksomheder potentielt kan miste omsætning eller lukke for at opretholde dette sikkerhedsniveau gennem lovmæssige reguleringer.

Der er en stor udfordring foran os på samfundsmæssigt plan, hvor der er mange ubesvarede spørgsmål og refleksioner samt dialoger som skal haves for at have en ide om, hvor og hvordan CSA potentielt kan implementeres, eller om det overhovedet skal gøres.

EU har igangsat NIS2 (Network and Information Security Directory 2), som er et EU-direktiv designet til at sikre nøgleinfrastruktur og tjenester mod nedbrud og cybertrusler via et højt bundniveau af ensartet cyber- og informationssikkerhed i hele EU. Dette skal være implementeret senest d. 17. Oktober 2024 (Europa Parlamentet, 2023). Der var en bred succes med implementeringen af GDPR, hvilket viser, at lovgivning og reguleringer af ikke kvantificerbare emner kan pakkes ned til standarder for at sikre policer, handlinger og sikkerhed på bredt plan. Det kan derfor argumenteres for, at disse lovgivninger har en positiv effekt på CSA.

4.2 Udvidelse af teknologiske forståelsesrammer

I dette speciale er Orlikowski og Gash (1994) teori omkring teknologiske forståelsesrammer anvendt til at undersøge om forståelsen og fortolkningen af CSA har indflydelse på forankringen i en organisation. Orlikowski og Gash (1994) teori tænker i grupper af interessenter, der deler en forståelsesramme, men nævner også kort, at forståelserne indenfor den samme ramme, kan have forskelligheder.
En relevant diskussion i denne sammenhæng vil være, om det er tilstrækkeligt at undersøge forståelsesrammer ud fra et gruppe-perspektiv.
Young m.fl. (2016) og Spieth m.fl. (2021) argumenterer for, at misalignment mellem områder i en gruppes fælles forståelsesramme er lige så problematisk som inkongruens blandt to gruppers forståelsesrammer. Dette kalder de for ramme inkonsistens (Spieth m.fl., 2021; Young m.fl., 2016). Dette gælder især ved arbejdet med en implementering af teknologi, hvor forståelser og fortolkninger af teknologien har indflydelse på implementeringen.

I den forbindelse, kan der argumenteres for, at det ville være relevant at lave en yderligere undersøgelse af flere grupper i Hjørring Kommune vedrørende udbredelsen/implementeringen af CSA. I denne rapport er der interviewet medarbejdere fra to grupper, men en yderligere undersøgelse af flere grupper kan være fordelagtig. En kommune er af naturlige årsager delt op i flere områder og afdelinger, hvilket også kommer til syne i denne rapport. Hvad der i denne sammenhæng også kommer til syne, er, at disse områder kan have forskellige forståelser af en teknologi og forskellige kulturer, der påvirker denne forståelse. Dog viser rapporten også, at der findes forskellige forståelser indenfor den samme gruppe, som det eksempelvis var tilfældet i gruppen med medarbejdere fra andre kommunale stillinger. Denne gruppe indeholder dog medarbejdere fra flere forskellige områder, såsom skoleområdet, handicapområdet og ældreområdet. Der kan argumenteres for, at en yderligere inddeling i eksempelvis disse områder, vil vise yderligere indsigter i forståelser for CSA. En sådan dybdegående undersøgelse vil give en dyb indsigt i, hvordan forståelsesrammerne for forskellige mindre grupper, eller individer, har indflydelse på udbredelsen af CSA.
Omvendt vil en sådan detaljeret analyse være tids- og ressourcekrævende. I tilfældet med Hjørring Kommune, drejer det sig om en stor organisation, som beskrevet i afsnit 1.4. Hvis forståelsesrammerne undersøges på individ niveau, eller i mindre grupper, kan der argumenteres for, at resultatet eventuelt ikke retfærdiggør brugen af ressourcer.
Der kan dog være en øvelse i, at lave en analyse af forståelsesrammer ud fra den rigtige størrelse af grupper, der viser en repræsentativ fordeling i organisationen. Hvad den rigtige størrelse så er, vil sandsynligvis afhænge af den specifikke kontekst.
I denne forbindelse, dukker en diskussion omkring, hvor meget CSA skal fylde i en organisation op. Vores undersøgelse viser, at det skal fylde mere i hverdagen hos alle, hvis forståelserne skal forenes, og have en positiv indflydelse på en forankring. Dette kan dog også skyldes, at vi anvender et teoretisk grundlag, der har til formål at undersøge specifikke IT-systemer om et IT begreb.
Omvendt viser den eksisterende litteratur, at angreb ikke fuldstændig kan forhindres (Hoeing m.fl., 2022). Da respondenter i denne rapport ser CSA som noget forebyggende, opstår der hermed et spørgsmål omkring, hvor meget energi og ressourcer, der skal anvendes til denne forebyggelse, hvis det alligevel er umuligt at forebygge. Der kan være argumenter for i stedet at anvende disse ressourcer på eventuelt at udarbejde en handleplan for, hvad der skal ske, når en trussel bliver en realitet.

4.3 Hvorfor kontekst i forhold til forståelsesrammer?

Domæneanalysen blev valgt, da det er en etnografisk analyse, som er defineret som *"It refers to the systematic examination of something to determine its parts, the relationship among parts, and their relationship to the whole."* (J. P. Spradley, 1979). Den etnografiske analyse bringer en ny vinkel, hvor forståelsesrammerne er en socio-kognitiv tilgang, som defineres: *"SCA is interested in the interconnections between knowledge, discourse and society while placing subjectivity in the centre of its framework"*(Gyollai, 2022).

Formålet ved domæneanalysen og den etnografiske tilgang, er, at det giver en systematisk gennemgang af, hvordan kulturen i forskellige dele af organisationen er, sammenlignet med kulturen på tværs af organisationen og relationen mellem dem. Denne relation gav unikke indsigter, som eksempelvis, hvordan strategien for databeskyttelsesteamet fungerer i forskellige kontekster og, hvordan den kan have indflydelse på forståelsesrammerne. Det kan argumenteres for, at uden domæneanalysen er det ikke nødvendigvis sikkert, at denne relation ville være fundet.

Denne relationsbaserede analyse kan derfor bringe andre indgangsvinkler end den subjektivcentraliserede analyse som forståelsesrammerne bringer.

Sættes dette i kontekst med tidligere diskuterede emner, såsom udvidelsen af teorien omkring teknologiske forståelsesrammer, kan der argumenteres for, at den etnografiske analyse viser de relationerne mellem forståelserne internt i grupperne. Analyserne af domæner og modenhed undersøger konteksten, hvori forståelsesrammerne skabes og formes, hvorfor de kan give en indsigt i disse og give en fordel i forankringen af CSA.

Det er værd at nævne, at disse analysevinkler ikke giver et endegyldgt svar på analyser af forståelsesrammer. Vi har valgt anvende disse metoder, da vi mener konteksten for forståelsesrammerne er relevant. Som nævnt tidligere, kan en anden relevant vinkel være det individuelle perspektiv beskrevet af Young m.fl. (2016) og Spieth m.fl. (2021).

5 | Refleksion

Dette projekt har gjort brug af den induktive metode, hvor dataen og informationen indsamlet har sat rammerne for medarbejdernes forståelse af CSA. En alternativ metode kunne være at bruge den deduktive metode, hvor projektet ville have haft hypoteser og klare forventninger til forståelsen af CSA hos medarbejderne inden dataindsamlingen. Den induktive metode i den ideelle verden gør at der ikke er en forudkonditionering inden indsamlingen af dataen, hvor det aktuelle billede var lidt anderledes, da gruppen har lavet et dybdegående litteraturstudie om emnet, hvorfor der var en hvis partiskhed, som kunne fordæmpes, da de tre gruppemedlemmer kunne holde hinanden oppe imod den induktive filosofi, som dataindsamlingen var bygget op omkring.
Der kan dog argumenteres for, at en forudkonditionering aldrig kan undgås. I dette projekt har vi dog bevidst arbejdet med dette, for at give undersøgelsen så lidt bias som muligt. Dette er eksempelvis gjort ved interviewguiden, udvælgelseskriterier for uddrag fra interviews og selve det, at vi er bevidste omkring vores position som undersøgere gennem projektet. Ligeledes har det været et fokus at mindske denne bias på bedst mulig vis, så resultaterne fra projektet er replikerbare.

Den induktive tilgang har belyst ikke forventelige synspunkter i dataen, specielt i forbindelse med kendskabet til CSA og det førnævnte dualitetsfænomen, samt den indflydelse en tredive minutters dialog med interviewpersonerne havde. Den induktive metode viste også fordele og ulemperne ved at have åbne spørgsmål til interviewet, da meget af dialogen ender i periferier og i dele som er uforventelige der kan gøre de sektioner irrelevante i forbindelse med undersøgelsen, hvis ikke intervieweren er god til at navigere dialogen i den rigtige retning. Et emne som ofte blev nævnt fra interviewpersonerne var GDPR, hvilket kunne forventes at være et mindre naturligt emne at påtale i forbindelse med CSA. Paradokset i dette projekts tilfælde er, at GDPR oftest blev påtalt i sådan en omfang at det hjalp interviewpersonerne med at forklare deres forståelse af et emne de havde lav viden omkring, inden GDPR blev lovmæssigt indført. Paradokset forekommer, da projektet undersøger interviewpersonernes og organisationens forståelse af CSA, at denne forklaring af GDPR og deres brug af det var valid data og gav unikke indsigter.
Styrken ved den induktive tilgang er altså, at den kan vise observationer, som ikke nødvendigvis var blevet opdaget, hvis vi som undersøgere havde ladet vores forudkonditionering være en større faktor i undersøgelsen.

Denne indsigt ville ikke have været en mulighed, hvis den deduktive metode var anvendt. Derimod er det forventeligt at dataindsamlingen havde været mindre abstrakt og mere specifik i forbindelse med deres rå forståelse af CSA. Desuden ville den deduktive metode også have en række hypoteser som skulle be- eller afkræftes, som ville gøre undersøgelsen mere målrettet fra start, hvor interviewguiden og interviewformen kunne have haft en anden natur, end den som blev udarbejdet. Af natur læner den deduktive metode sig mere op af kvantitativt data, hvor induktiv arbejder mere i den kvalitative ende. Essensen af den deduktive metode ville i dette projekt udføre sig til at der skulle være en række kasser som skulle tjekkes af, for at be- eller afkræfte hypoteser, som ville kunne give et smalt, men præcist svar på projektets forskningsspørgsmål. Da CSA er et nyere og ikke velkendt begreb, var den induktive metode mere passende i forbindelse med den størrelse CSA har på nuværende tidspunkt.

6 | Fremtidigt arbejde

Denne undersøgelse har vist, at der findes forskellige forståelsesrammer i den undersøgte organisation. Disse forståelsesrammer er præget af kulturen og modenheden i organisationen. Ligeledes viser undersøgelsen, at disse forståelser har en indflydelse på forankringen af CSA i en organisation. Det næste oplagte skridt i forskningen, ville derfor være at undersøge, hvordan forskelle i forståelsesrammer kan forenes for at skabe et bedre fundament for en forankring af CSA.

Herefter kunne det være relevant at undersøge CSA kan kvantificeres, måles og gives værdier som kan bearbejdes og fortælle historier om både individer, organisationer og på længere sigt samfund og lande. Denne måling vil derfor kunne være et startspunkt, når der bliver undersøgt om der skal investeres i det og i hvilken grad der skal investeres i CSA. Denne måling vil også kunne skabe kongruens på tværs af individer, hold, organisationer og markeder, hvor der kan skabes generelle afprøvede og succesfulde øvelser, tests og træninger for at opretholde og forøge niveauet af CSA på diverse områder. Det skal understreges, at bare fordi der er en metode til at måle niveauet af CSA, betyder det ikke at ondsindede aktører ikke finder nye muligheder og vinkler for angreb, for det er en kontinuerlig proces, som ikke forventes at stoppe i den nære fremtid. Dette vil blot give et indblik i, hvor effektive nuværende virksomheder er, så de kan komme på niveau med de nuværende angreb de oplever, for efterfølgende at følge i takt med de ondsindede aktøreres niveau og udspekulerede planer til angreb og vokse i sammenspil med angrebene.

Efterfølgende kunne det fremtidige arbejde indeholde udviklingen af et bredt rammeværk, som indeholder en forundersøgelse til at påvise det nuværende niveau et område er på, efterfølgende et ønsket punkt som området ønsker at ramme, og hvordan det vedligeholdes. Dette vil også indeholde den optimale træningsmetode, da CSA træning på nuværende tidspunkt er reduceret til e-læringsværktøjer og kurser, hvor det ikke er let tilgængeligt, hvor meget hvert individ får ud af hver træningsgang og afslutning af et kursus eller træningsforløb. Det næste skridt ville være at finde den optimale metode at vedligeholde niveauet efter træningen. Påtale og imødekomme den førnævnte dualitet af forståelse, de optimale kulturelle forhold, en accept for at fejl kan forekomme og ned på et dialogbasis, samt en forståelse af at det ikke handler om; om der sker brud, men hvornår der kommer brud.

Et rammeværk som førnævnte, vil i sidste ende have til formål at ændre adfærden hos individer. I den forbindelse vil det være relevant at undersøge, hvordan denne adfærd kan ændres i forhold til CSA. Da CSA er et nyt begreb, der findes mange forståelser af, som denne undersøgelse viste. Det viste sig dog også, at der også fandtes manglende forståelser af begrebets eksistens. Det kunne derfor tænkes, at det vil kræve ekstra opmærksomhed i arbejdet, som eksempelvis Kahneman (2011) beskriver i hans teori. Dette kunne eksempelvis være et interessant område at undersøge videre i fremtidigt arbejde.

Et mere specifikt område der kan videreundersøges, er, at kigge på hvordan de forskellige arbejdsområder i en virksomhed arbejder med cybersecurity og CSA, for efterfølgende at få indsigt og sammenligne deres succeser og potentialer. Dette ville potentielt kunne finde forskellige kulturelle og forståelsesmæssige lig- og uligheder.

Det er værd at nævne at samtlige punkter under dette potentielle rammeværk er en fremtidig undersøgelse i sig selv, da litteraturstudiet Hoeing m.fl. (2022) viste at der ikke var et væld af empirisk data på diverse områder som rammeværket indeholder.

7 | Konklusion

Gennem en metodisk analyse af projektets empiri, har dette projekt til formål at besvare det indledende forskningsspørgsmål, der beskrives som følgende:

Hvilken betydning har forståelse for cybersecurity awareness på, hvordan cybersecurity awareness forankres i en organisation?

For at besvare forskningsspørgsmålet, blev der primært analyseret på baggrund af teorien omkring forståelsesrammer. Dette bliver understøttet af analysen af kulturen og CSA modenhed ved at undersøge konteksten hvori forståelsesrammerne opstår. Denne undersøgelse har gjort det muligt at drage nedenstående konklusioner.

Analysen af forståelsesrammerne af cybersecurity awareness undersøgt i Hjørring Kommune har vist, at der findes inkongruente forståelsesrammer. Det kan konkluderes, at disse inkongruenser har en negativ indflydelse på det foregående arbejde med at udbrede og forankre CSA i organisatioen.

Analysen af domæneanalysen i Hjørring Kommune undersøgte det kulturelle element som en understøttende faktor til at behjælpe med forståelsesrammerne og undersøge konteksten for disse rammer. Ud fra denne analyse kan der konkluderes at en understøttelse af forståelsesrammerne gennem kulturen kan være en organisatorisk opmærksomhed til at forhøje niveauet af cybersecurity awareness både på individuelt plan og på tværs af organisationen.

Baseret på analysen af Hjørring Kommunes awareness modenhedsniveau kan der konkluderes, at ud fra den indsamlede empiri, kan Hjørring Kommune places mellem perception og protection niveauet i Fertig m.fl. (2020)'s teoretiske modenhedsniveauer. Som tidligere beskrevet er dette baseret på deres nuværende omgang med cybersecurity awareness på et organisatorisk niveau.
Det kan konkluderes at awareness modenhed kan have indflydelse på forståelsen af cybersecurity awareness. Den kan give et overblik over organisationens nuværende situation, samt give et indblik i hvordan nedbrydelsen af organisatoriske barrierere kan skabe en udvikling i awareness modenhedsniveauet.

Der er en kulturel enighed om, at cybersecurity awareness er et presserende problem, som er generelt accepteret. Dog er der en generel tendens til at nedprioritere CSA hos de individuelle medarbejdere, hvorfor ansvaret ofte bliver lagt hos IT-afdelingen. Dette er et bevis på, at der er en generel uenighed mellem de individuelle medarbejdere og organisationens IT-afdeling angående forventningsafstemningen og forståelsesrammerne når det kommer til cybersecurity awareness.

Det kan konkluderes, at den kulturelle og modenhedsmæssige kontekst som forståelsesrammerne befinder sig i, har indflydelse på, hvordan disse rammer opstår og formes. En ændring eller et fokus på disse organisatoriske opmærksomheder har derfor en implicit indflydelse på forståelsesrammerne.
Det kan yderligere konkluderes at forståelsesrammerne har en indflydelse på arbejdet med at forankre CSA i en organisation.

Litteratur

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour and Information Technology*, *33*(3), 237–248. https://doi.org/10.1080/0144929X.2012.708787

Alhashmi, A. A., Darem, A., Abawajy, J., Alhashmi, A. A., Darem, A., & Abawajy, J. H. (2021). *Taxonomy of Cybersecurity Awareness Delivery Methods: A Countermeasure for Phishing Threats* (tekn. rapp. Nr. 10). www.ijacsa.thesai.org

Alhuwail, D., Al-Jafar, E., Abdulsalam, Y., & Alduaij, S. (2021). Information Security Awareness and Behaviors of Health Care Professionals at Public Health Care Facilities. https://doi.org/10.1055/s-0041-1735527

Alqahtani, M. A. (2022). Cybersecurity Awareness Based on Software and E-mail Security with Statistical Analysis. *Computational Intelligence and Neuroscience*, *2022*. https://doi.org/10.1155/2022/6775980

Alsulami, M. H., Alharbi, F. D., Almutairi, H. M., Almutairi, B. S., Alotaibi, M. M., Alanzi, M. E., Alotaibi, K. G., & Alharthi, S. S. (2021). Measuring awareness of social engineering in the educational sector in the kingdom of saudi arabia. *Information (Switzerland)*, *12*(5). https://doi.org/10.3390/info12050208

Alzahrani, L. (2021). *Statistical Analysis of Cybersecurity Awareness Issues in Higher Education Institutes* (tekn. rapp. Nr. 11). www.ijacsa.thesai.org

Arain, M. A., Tarraf, R., & Ahmad, A. (2019). Assessing staff awareness and effectiveness of educational training on IT security and privacy in a large healthcare organization. *Journal of Multidisciplinary Healthcare*, *12*, 73–81. https://doi.org/10.2147/JMDH.S183275

Back, S., & Guerette, R. T. (2021). Cyber Place Management and Crime Prevention: The Effectiveness of Cybersecurity Awareness Training Against Phishing Attacks. *Journal of Contemporary Criminal Justice*, *37*(3), 427–451. https://doi.org/10.1177/10439862211001628

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers and Security*, *39*(PART B), 145–159. https://doi.org/10.1016/j.cose.2013.05.006

Bryman, A. (2012). *Social Research Methods* (tekn. rapp.).

Canham, M., Posey, C., & Constantino, M. (2022). Phish Derby: Shoring the Human Shield Through Gamified Phishing Attacks. *Frontiers in Education*, *6*. https://doi.org/10.3389/feduc.2021.807277

Cyber Security Degree. (2023). History of Cyber Security - Cyber Security Degree. https://cybersecurity.degree/resources/history-of-cyber-security/

Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2022). Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks. *Education and Information Technologies*, *27*(4), 4729–4752. https://doi.org/10.1007/s10639-021-10806-7

Europa Parlamentet. (2023). The NIS2 Directive: A high common level of cybersecurity in the EU | Think Tank | Europa-Parlamentet. https://www.europarl.europa.eu/thinktank/da/document/EPRS_BRI(2021)689333

Fertig, T., Schütz, A., Weber, K., & Müller, N. (2020). *Towards an Information Security Awareness Maturity Model* (tekn. rapp.). http://www.springer.com/series/7409

Foro Económico Mundial., Marsh & McLennan., SK Group. & Zurich Insurance Group. (2022). *The global risks report 2022*. World Economic Forum.

Gyollai, D. (2022). The sociocognitive approach in critical discourse studies and the phenomenological sociology of knowledge: intersections. *Phenomenology and the Cognitive Sciences*, *21*(3), 539–558. https://doi.org/10.1007/s11097-020-09704-z

Hepp, S. L., Tarraf, R. C., Birney, A., & Arain, M. A. (2018). Evaluation of the awareness and effectiveness of IT security programs in a large publicly funded health care system. *Health Information Management Journal*, *47*(3), 116–124. https://doi.org/10.1177/1833358317722038

Hoeing, M., Jeppesen, D., & Winthereig, H. (2022). *Cybersecurity Awareness i et organisatorisk perspektiv* (tekn. rapp.).

Jensen, M. L., Durcikova, A., & Wright, R. T. (2019). Using susceptibility claims to motivate behaviour change in IT security. *European Journal of Information Systems*, 1–19. https://doi.org/10.1080/0960085X.2020.1793696

Kahneman, D. (2011). *Thinking Fast and Slow*.

Kaspersky. (2023a). What is Social Engineering? | Definition. https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering

Kaspersky. (2023b). What is Spear Phishing? | Definition and Risks. https://www.kaspersky.com/resource-center/definitions/spear-phishing

Li, H., Yoo, S., & Kettinger, W. J. (2021). The Roles of IT Strategies and Security Investments in Reducing Organizational Security Breaches. *Journal of Management Information Systems*, *38*(1), 222–245. https://doi.org/10.1080/07421222.2021.1870390

Merriam-Webster. (2023). Phishing Definition & Meaning - Merriam-Webster. https://www.merriam-webster.com/dictionary/phishing

Orlikowski, W. J., & Gash, D. C. (1994). *Technological Frames: Making Sense of Information Technology in Organizations* (tekn. rapp.).

Pósa, T., & Grossklags, J. (2022). Work Experience as a Factor in Cyber-Security Risk Awareness: A Survey Study with University Students. *Journal of Cybersecurity and Privacy*, *2*(3), 490–515. https://doi.org/10.3390/jcp2030025

Sharif, K. H., & Ameen, S. Y. (2020). A Review of Security Awareness Approaches with Special Emphasis on Gamification. *3rd International Conference on Advanced Science and Engineering, ICOASE 2020*, 151–156. https://doi.org/10.1109/ICOASE51841.2020.9436595

Shojaifar, A., & Fricker, S. A. (2020). *SMEs' Confidentiality Concerns for Security Information Sharing* (tekn. rapp.).

Spieth, P., Röth, T., Clauss, T., & Klos, C. (2021). Technological Frames in the Digital Age: Theory, Measurement Instrument, and Future Research Areas. *Journal of Management Studies*, *58*(7), 1962–1993. https://doi.org/10.1111/joms.12720

Spradley, J. (1979). The Ethnographic Interview.

Spradley, J. P. (1979). The Ethnographic Interview.

The Global Risks Report 2023 18th Edition. (2023). www.weforum.org

Trim, P. R., & Lee, Y. I. (2019). The role of B2B marketers in increasing cyber security awareness and influencing behavioural change. *Industrial Marketing Management*, *83*, 224–238. https://doi.org/10.1016/j.indmarman.2019.04.003

Wang, K., Guo, X., & Yang, D. (2022). Research on the Effectiveness of Cyber Security Awareness in ICS Risk Assessment Frameworks. *Electronics*, *11*(10), 1659. https://doi.org/10.3390/electronics11101659

Weill, P. (2004). *All rights reserved* (tekn. rapp. Nr. 1). http://mitsloan.mit.edu/cisr

Wolfswinkel, J. F., Furtmueller, E., & Wilderom, C. P. (2013). Using grounded theory as a method for rigorously reviewing literature. https://doi.org/10.1057/ejis.2011.51

Young, B., Mathiassen, L., & Davidson, E. (2016). Inconsistent and incongruent frames during it-enabled change: An action research study into sales process innovation. *Journal of the Association for Information Systems*, *17*(7), 495–520. https://doi.org/10.17705/1jais.00432

A | Bilag

A.1 Interview - Skolelærer

Interview starter

[00:00] Heine: Så hvis du vil have lyst til at starte, måske med at fortælle lidt om dig selv og hvad du laver?

[00:06] Skolelærer: Ja, det vil jeg gerne. Jeg hedder som sagt Skolelærer (Anonymiseret, jeg er 29 år gammel, og jeg arbejder på Hjørringskolen som lærer i en specialklasse. Det vil sige en klasse, hvor det er børn med ADHD og andre diagnoser. Det har jeg gjort i 4 år. Og faktisk fra mandag næste uge, der har jeg fået en ny job hos KMD inde i Aalborg, så der skifter jeg faktisk lidt hat. Og ikke skal være lærer længere, men supportkonsulent hos min uddannelse. Ja, og jeg har været lærer i 4 år. Jeg blev færdiguddannet for 4 år siden, så jeg har egentlig bare været i gang lige siden.

[00:48] Martin: Spændende.

[00:50] Heine: Så i forhold til introduktionen og det der var lige før her, vil du så skrive 3 ord ned, når du hører ordet Cybersecurity?

[01:02] Skolelærer: Jeg har chatten åbent, hvis det er.

[01:05] Heine: Ja, det gør du bare.

[01:07] Skolelærer: Altså 3 ord?

[01:09] Martin: Ja, når vi siger Cybersecurity Awareness, så er det 3 ord, du kommer til at tænke på.

[01:20] Heine: Okay, og hvad kan man sige, hvorfor har du så valgt de her 3 ord? Nu har der jo mange forskellige, man kunne have valgt, men hvorfor er det lige ind på de her 3?

[01:39] Skolelærer: Jeg tror, at det er de 3 primære ting, jeg tænker i forhold til det. Cybersecurity for mig er i hvert fald noget med at forebygge og være sikker på, at man er på forkant med de ting, der kan ske i organisationen, som vi er i. Men det handler også om, at der er nogen, der tager ansvar for at få fulgt op på det og sørge for, at sikkerheden er i orden.

[02:04] Heine: Når du kommer til dit kendskab til Cybersecurity, hvordan er det så?

[02:09] Skolelærer: Jeg tænker egentlig, det er ikke sådan mega stort, men det er da noget, der berører mig i hverdagen. For eksempel sådan noget som password, det er jo noget, der har rigtig stort fokus på, at vi ret ofte skal ændre og lave om på. Tofaktor genkendelse er også noget, vi får besked på, om det er en god idé at have i forhold til vores maskiner, med GDPR og alle de informationer, vi har på vores maskiner, og vi også har på vores drev. Så er der jo rigtig mange informationer derinde omkring vores børn og sådan noget, der har meget følelse om det. Så det synes jeg jo egentlig, giver rigtig god mening, at der er stort fokus på at ændre vores passwords og sådan nogle ting.

[02:56] Martin: Når vi siger cyber security awareness, hvad tænker du så? Er det noget, du har hørt før?

[03:04] Skolelærer: Når jeg hører det, så tænker jeg jo, at det er det her med at være bevidst om, at det er noget, der er vigtigt. Det tror jeg faktisk ikke, at det er mange, der er. Dem, som måske har en lille smule IT-snilde, de ved nok godt, hvad det handler om. I min organisation, der vil jeg tro, at 80% af vores stab, vil nok ikke helt vide, hvad det handler om. Det er bare slag på tasken.

[03:35] Martin: Er det noget, du er bevidst om i din hverdag, eller noget, du er bevidst tænker over?

[03:43] Skolelærer: Ja, det synes jeg. Det synes jeg i hvert fald, jeg gør mere nu, end jeg gjorde for fem år siden.

[03:48] Martin: Hvordan?

[03:50] Skolelærer:Det er bare noget, der er en stor del af alles hverdag. Man hører tit om, at der er leaks og hacking angreb forskellige steder. Det er bare noget, vi bliver nødt til at tage stilling til i dag, tænker jeg. Fordi det er så stort, og det er så udbredt.

[04:07] Martin: Hvordan er det så, at det kommer til syne i din hverdag? Er det noget specielt, du gør?

[04:15] Skolelærer: Jeg tror, jeg er mere bevidst om, hvilke søgemaskiner jeg bruger, når jeg browser på nettet. Jeg er bevidst om, hvilke apps jeg giver tilladelse til, på min telefon for eksempel. Jeg er bevidst om, hvad jeg siger, hvornår, i forhold til, om der er nogen ting, der optager det, jeg siger. I forhold til algoritmer og sådan nogle ting.

[04:39] Heine: Hvad med i forhold til på arbejdspladsen? Er det noget, I generelt snakker om?

[04:48] Skolelærer: Det er meget lidt. Jeg har en kollega, som også godt kan ligge til. Vi snakker engang imellem om det, men det er ikke noget, jeg snakker en hel masse med mit team om. Det er heller ikke noget, jeg generelt snakker med mine kollegaer om. Det er meget lidt i hvert fald.

[05:06] Heine: Når det kommer til Cyber Security Awareness, så lavede vi et litteraturstudie på sidste semester. Der var en masse ting, som kunne hjælpe med at forhøje Cyber Security Awareness. Du er kun så stærk som det svageste led. Menneskelig fejl er 90Hvor de er lækkere, og de har targetet, fordi svagheden ligger. Hvor en kontinuerlig snak om det bliver en mere fast del af kulturen. Det er en rigtig god måde at afhjælpe det på. Hvad tænker du til det, når du hører det? Er det noget, du kan genkende til, når det kommer til din hverdag?

[05:55] Skolelærer: Nej. Ikke i høj grad i hvert fald. Det synes jeg ikke.

[06:02] Heine: Tror du, det kunne være på grund af, at folk enten ikke tænker over det. Hvor vigtigt det er, eller om det måske er en... Fordi det er noget teknisk noget, selvom det i undergrunden egentlig ikke er. Men måske fordi de tror, det er noget teknisk, og måske noget lidt fluffy noget. Så er det noget, de vil se hen over.

[06:21] Skolelærer: Jeg tror i høj grad, det er det. At man ikke lige helt ved, hvad det er. Er det noget teknisk, eller er det ikke noget teknisk? Har jeg egentlig forståelse, eller har jeg viden omkring det? Nej, det har jeg måske nok ikke. Så bliver det nedprioriteret på en eller anden måde. I forhold til de andre ting, der foregår i løbet af sådan en hverdag.

[06:39] Heine: Tror du, det er en aktiv ting, eller tror du mere, det er sådan en passiv ting?

[06:44] Skolelærer: Jeg tror nok faktisk, mere det er en passiv ting. Umiddelbart.

[06:50] Martin: Er det noget, du synes, der er vigtigt i din hverdag, dit arbejde? Fylder det meget, eller burde det fylde meget?

[07:01] Skolelærer: Det fylder jo ikke meget. Det er nok mere i min underbevidsthed, tror jeg. Jeg tror ikke, jeg synes, det skal fylde mere for mig. Men jeg tror måske, at jeg synes, det skal fylde mere på bredt plan. At der er flere, der er klar over det, og flere, der er med på, hvordan vi gør for at forhindre de ting.

[07:20] Martin: Tror du så, at der er forskellige forståelser af Cyber Security Awareness? Eller er det bare fordi, man simpelthen ikke kender til det? Eller er det fordi, der er nogen, der måske tænker, at det tager IT-afdelingen sig af?

[07:36] Skolelærer: Det tror jeg, der er mange her, der gør. Jeg tror, der er mange, der tænker, at vores IT-mand, han styrer det der. Faktisk. Det er nok de 80 procent, der er, som jeg nævnte før.

[07:48] Heine: Tror du, det er noget, der kunne gavne din afdeling? At det måske var noget, hvor alle samarbejdet om at forhøje det her niveau. At det måske var noget, man bare snakkede om en gang imellem. At det kommer lidt mere brutal, og at det bliver lidt mere kvantificeret. Fremfor at det altid er sådan noget fluffy, men jeg ved ikke helt, hvad det er for noget.

[08:12] Skolelærer: Det tror jeg, det er kun bare det her med at få det afmystificeret på en eller anden måde. Sådan at alle, mere eller mindre, ved, hvad det handler om. Det tror jeg, jeg ville gøre meget ved, at det var noget, man også kom til at snakke om. Og noget, der var mere fokus på hos alle medarbejdere. Og dem, som har en idé om, hvad det handler om.

[08:32] Martin: Hvordan tror du, at man kunne gøre det bedst? Tror du, det er sådan nogle træningsprogrammer eller workshops?

[08:42] Skolelærer: Det er et svært spørgsmål. Det er et rigtig svært spørgsmål. Også fordi, at der er mange, som i det her fag synes tiden er knap. Og det der med at få de rigtige ting ind. Også specielt, når det er noget, der måske skal foregå ud over den hele arbejdstid. Så er det faktisk rigtig, rigtig svært at finde ud af, hvordan overledes kan man det. Men det kunne da sagtens være... Altså det der med bare lige at sidde med et program, den ved jeg ikke. Men det med at få belyst det på en eller anden måde. At der er nogen, der kommer og fortæller om det. Sætter fokus på det på en anden måde måske. Det tror jeg godt, man kunne nå langt med.

[09:24] Martin: Også med at få mere information om det måske. Det er måske lidt svært, fordi man ikke selv får en direkte værdi af at gøre det. Men mere sådan, at man skal se værdien for en organisation.

[09:38] Skolelærer: Også kan man sige... Hvis der kommer sådan nogle informationer, som der jo gør engang. Så er det jo også ofte noget, der kommer ind på AULA, vores platform. Hvor det ligger i en oversigt eller i en besked. Der er jo nogen, når de læser, om der står noget med cyber eller der står noget med IT. Så er der nogen, der allerede er videre til næste besked. Så det der med, at det sådan er et eller andet, der bliver stablet på benene. Hvor det er en eller anden person, der kommer og ligesom gør opmærksom på det. Og fortæller om det. Det tror jeg i hvert fald er en bedre vej end det andet.

[10:14] Dylan: Som lærer, så er der vel også... Altså mere og mere digitalisering i hvert fald i forhold til børnene. Altså de lærer også at bruge det her udstyr. Altså bliver det et emne, der bliver taget op nogensinde. Altså man snakker om, at internet er måske lidt halvfarligt. Udover bare klamme mænd.

[10:35] Skolelærer: For mit vedkommende ja. Jeg er samfundsfagslærer blandt andet. Og jeg er også engelsklærer. Og det er noget, jeg tager fat i af og til. Men det er ikke noget, der sådan fastlagt i boende ligger i nogen former. For årsplaner eller noget som helst. Så det er noget, jeg tænker, man skal selv have lysten til. Ligesom at tage det op med klassen. Men jeg synes jo, det er enormt vigtigt. Fordi som du selv siger, internettet er bare et farligt sted. Men det er ikke noget, alle gør langt fra. Jeg tror heller ikke, det er ret mange her på stedet, der tager det op. I deres undervisning aktivt. Selvom det er enormt vigtigt.

[11:15] Dylan: Men det kommer nok af et sted fra... Uvidenhed eller at man måske ikke selv føler sig komfortabel nok i de her ting. Så det kunne jo være en eller anden vej ind til, at man ville italesætte det. Og sige, det hjælper også eleverne. Det er nok der, meget motivation også kommer fra.

[11:33] Skolelærer: Det i hvert fald tror jeg er en god måde at motivere lærerne på os. Til ligesom at blive klogere på det. Med henblik på at kunne give det videre. Det er også en vigtig ting at give eleverne med.

[11:43] Martin: Det er nok det, der også er nøglen at finde et eller andet, der kan motivere folk til at...

[11:53] Skolelærer: Jeg tror i hvert fald lige med lærer, sikkert med rigtig mange andre mennesker også. Det skal give mening. Der skal være en idé med, at vi sidder over to timer på at høre om cyber security eller hvad nu.

[12:08] Heine: Og det er det, der er lidt sjovt ved fænomenet. Fordi det er ret svært at kvantificere. Du ved ikke, hvornår du er aware. Du ved ikke, hvornår du er god nok fagligt. Og når der så kommer et angreb, så ved du så overhovedet, om det er et angreb, der kommer. Ved du, om det er en form for phishing mail, der kommer ud? Har du den viden, at du kan identificere det? Så du kan få det behandlet rigtigt, ikke?

[12:38] Skolelærer: Ja. Det er svært at måle vej, hvornår man er det rigtige sted.

[12:43] Heine: Det er også interessant, fordi det er en kontinuerlig proces. I forhold til det her område her, hvad vil du så mene, at det betyder at være aware i forhold til cyber security? Ud fra din opfattelse?

[12:56] Skolelærer: Jeg tror bare, at det er, at man er bevidst om, at uanset hvad du laver på nettet nærmest, så er der nogen, der tracker dig, der er nogen, der ved, hvad du laver, og der er nogen, der kæmper om at få din information, altså at få din opmærksomhed. Og den går til højeste udbyder, kan man sige. Det er i hvert fald nogle af de ting, som jeg sætter fokus på, når vi snakker om det. Og så hele tiden det her med, at det er bare nemt at komme i klemme muren til, hvad man laver online. Alt det her med anonymiteten og sådan noget. Så det er noget, jeg har rigtig stort fokus på. Også i forhold til nu nævnte de også TikTok og apps og sådan nogle ting. Altså hvordan navigerer man dem bedst, det er helt klart sådan noget, som jeg sætter fokus på.

[13:41] Martin: Arbejder I med noget sensitive data eller sådan noget i hverdagen? Jeg ved ikke om I... Altså det gør vi jo, fordi vi har jo... I kvæg af, at vi har de elever, vi har, så skriver vi jo ofte nogle ICS-skemaer eller udtalelser, og der er det jo ofte nogle meget personfølsomme med både ting, vi skriver, men også vurderinger, vi laver. Og alt det, vi laver, ligger som set på vores Chromebooks lokalt, men også i vores Google Drive. Ja. Så på daglig basis har vi med personfølsomme oplysninger at gøre, det vil jeg sige.

[14:21] Martin: Okay. Så der er dele i arbejdsdagen, hvor cybersecurity og sådan noget, det er faktisk ret kritisk?

[14:30] Skolelærer: Det kan man sige. Uden tvivl.

[14:35] Heine: I forhold til den her information, kan man sige, ved hvor meget kendskab har du så til, hvordan det bliver sendt og opbevaret og håndteret i forhold til din arbejdsgang?

[14:47] Skolelærer: Det er faktisk ikke voldsomt meget.

[14:53] Heine: Så hvis en ondsindet aktør får fat i dine login-oplysninger, ved du så, hvad for noget data han vil have adgang til, og hvor dybt han er, som vil kunne gå ind i det rabbit hole, der hedder dine login-oplysninger i jeres IT-systemer?

[15:08] Skolelærer: Ja, det tror jeg, jeg har en rimelig god idé om. Han vil jo have adgang til alt, hvad mine elever har at gøre, kan man sige. Og igen, der ligger en masse ting, og han vil egentlig også have adgang til mange af de sagsakter, der ligger omkring de her børn, som jeg har adgang til.

[15:27] Heine: Du kan ikke se andre klassers børn, for eksempel?

[15:33] Skolelærer: Jeg kan ikke se noget, nej. Jeg har tilknyttet min klasse, kan man sige, så det er dem, jeg egentlig har adgang til, hvis man kan sige det sådan.

[15:43] Dylan: Er det unikt, når du har en speciel klasse, at der er mere personfølsom data, end der vil være i en almindelig klasse, eller hvordan? For du siger, at du giver sagsakter, er det noget, der følger alle elever, eller er det kun på special klasse?

[15:57] Skolelærer: Det følger de elever, hvor der er noget, kan man sige, men i kraft af, at vi har de børn, vi har, så er der bare ofte flere ting omkring dem, end der er. Og ikke for at sige, at der ikke også er børn som vores i almen, det er der jo. Men det er bare tungere børn, hvis man kan sige det sådan. De forstår, hvad jeg mener. Der er næsten altid rigtig meget historik, og rigtig mange forskellige dokumenter og sådan noget, der følger med.

[16:33] Heine: Vi har kørt lidt rundt om det, men i forhold til din arbejdsdag, hvornår, og i hvilke dele er det så, hvor cybersecurity og Awareness-delen kommer til syne?

[16:46] Skolelærer: Jamen det er jo i de dele, hvor man kan sige, at jeg ikke har undervisning, hvor jeg sætter mig ned, og jeg skal skrive et eller andet, en underretning eller en udtalelse eller et ICS, og skal have sendt det et eller andet sted hen, som oftest er ekstern, uden for vores organisation, kan man sige.

[17:09] Heine: Og i forhold til, nu har du måske selv lidt interesse for cybersecurity, kan man sige, er det noget, du har fået træning i, i forhold til alt den viden, du har nu her?

[17:23] Skolelærer: Nej, det jeg ved, det er noget, jeg selv har holdt frem til eller har undersøgt. Og ja, der er ikke noget fra skolens side eller noget som helst.

[17:40] Martin: Spændende.

[17:43] Skolelærer: Meget.

[17:44] Heine: Ja, når det kommer til det her cybersecurity og Awareness og at det er lidt fluffy, tror du så, at vi var lidt over det før, men hvis det ligesom blev italesat på den rigtige måde, tror

du, at i og med du siger, at læreren skal kunne forstå, eller de skal have et eller andet ud af det, tror du, det er noget, man vil kunne formidle til dem på en måde, selvom de faktisk ikke ville få et resultat, de kunne tage med hjem og sige, okay, nu behøver vi ikke tænke over det mere, men at det er sådan en kontinuerlig proces, tror du, det er noget, man vil kunne overvinde dem om, og så ligesom kunne købe ind i, så de ville kunne ændre deres adfærd?

[18:29] Skolelærer: Ja, det tror jeg godt, men igen, det er fandme et svært segment at overbevise om ting, og det er bare virkelig meget det her med, at det skal give mening. Der skal være en mening med det, og jeg tænker netop det, vi talte om før, at hvis man kan vinkle det på en sådan måde, at det jo egentlig også er for børnene skyld for at gøre dem klogere på det, at fange dem tidligt, hvis man kan sige det, så de bliver bevidste om, hvordan man undgår, eller man forsøger for at blive her tænkt, så tror jeg faktisk, det er en rigtig god vinkel. Men det er selvfølgelig stadigvæk, tror jeg selvsagt, at dem, der er mere IT eller teknik interesseret, de vil nok tage det mere til sig, end Hans Christian på 67, som går på pension om 3 år, hvis I kan følge mig i den. Men jeg tror, det er helt klart vejen at gå, det skal give mening, og det skal give mening på en eller anden måde nu og her, selvom det selvfølgelig også giver mening at passe på sine informationer i organisationen.

[19:30] Martin: Det er lidt den klassiske problemstilling med, hvordan fanden får man dem til at...

[19:40] Heine: En klassisk bekymring for mange, der skal til at integrere som cybersecurity, det er noget, vi har set fra vores litteraturstudie, vi lavede sidste semester også, det er, at mange kan godt se det lidt som en hemsko, at det er lidt en forhindring, at de skal igennem nogle af de her barriere med to faktorer, og VPN og login og passwords og alt det der, og så kunne det måske give dem en form for mæthed, og få dem lidt træt af hele processen, og så måske miste det overordnede overblik over sikkerheden og hvor vigtigt den rent faktisk er, fordi det måske kan være en forhindring i deres daglige arbejde. Tror du, det er noget, der også kunne få lærerne eller måske dine kolleger til at være modstandere af implementeringen af nogle af de ting?

[20:38] Skolelærer: Det er der helt sikkert nogen, der vil. Der er jo nogle, hvor det er de mindste ændringer i det, man plejer at gøre. Der kan være træls. Hvis det er noget, man i forvejen har lidt svært ved, så jo, det ville det da sikkert, men det er jo også noget, der forholdsvis er uskyldigt, så jeg tror egentlig, at man godt kunne implementere det, og så ville der være nogen, der brokker sig, og så ville det gå over. Det kunne jeg godt forestille mig. Jeg tror ikke, at det er noget, der ville vedvarende være bekymringer eller irritationer omkring. Også hvis man snakker om, hvorfor er det, vi gør det.

[21:17] Heine: Okay, måske et lidt anderledes spørgsmål. I forhold til pensum og til en årsplan, tror du så, at det kunne være noget, som måske skulle implementeres i noget undervisning? Så snakker man også om fx personlig økonomi, skat og økonomi og hvordan man skal strukturere det. Hvordan tror du, at cybersecurity kunne være på samme niveau?

[21:43] Skolelærer: Det tror jeg godt, det kunne med tiden, og måske også allerede nu. Vi lever bare i en tid, hvor flere og flere ting digitaliseres, og lige pludselig, så er der jo ikke ret mange ting, vi gør fysisk længere. Så helt sikkert, så ville det da i min optik tage en plads sammen med de ting der. Og det er jo let for mig at sidde og sige, fordi jeg gør jo lidt af det i forvejen, kan man sige. Men ja, hvis I spørger mig, så ja. Uden tvivl.

[22:15] Martin: Ja, enigt. Jeg forstår det heller ikke.

[22:19] Heine: Har I noget andet end det sidste?

[22:21] Dylan: Nej, det tænker jeg ikke.

[22:23] Heine: Så en sidste lille øvelse. Hvis du vil skrive tre ting ned, som du tager med fra det her interview, som du måske vil tænke lidt mere over, eller det må gerne være det samme, men nogle overvejelser, eller et eller andet, du har fået ud fra den her lille snak her. Lige skriv det i chatten, så kan vi få det bogført.

[22:43] Skolelærer: Jeg tænker lige. Er det okay?

[22:45] Heine: Ja, det er helt okay.

[22:47] Martin: Det er også færre, hvis du kun kan tænke på et eller to. Det er mere bare sådan, om der er noget vildt, som du lige har tænkt over, mens vi snakkede.

[22:55] Skolelærer: Der var i hvert fald lige lidt der.

[23:21] Heine: I forhold til de ting her, hvad fik jeg til at tænke over dem i forhold til vores lille snak her?

[23:26] Skolelærer: Jeg tror lige det der med vidensdeling, det kom faktisk lige fordi, at vi jo er nogen, som egentlig sidder med lidt viden, men egentlig ikke rigtig sådan, som vi også sagde, vi får ikke rigtig snakket om det. Der kunne jeg måske godt, eller det kunne mine kollegaer måske også godt, tage til den, og så lige få snakket lidt omkring det, og egentlig finde ud af, hvor folk står i det. Og så det sidste, det var jo i forhold til det, vi snakkede om, at hvis man skal i gang med at implementere eller gøre folk klogere på det, så er det i hvert fald bare vigtigt, at det ikke er en besked på AULA, men at det ligesom er et eller andet, der bliver gjort, og noget, der har et islet, der giver mening i forhold til, hvorfor sidder vi og hører eller bruger to timer på det her.

[24:13] Martin: Det hænger også lidt sammen med det her med, at du skrev ansvar til at starte med. Også med at det ikke kun er IT-afdelings ansvar at beskytte organisationen, men at det faktisk også er det her med, at IT-systemerne faktisk fungerer ret godt, men at det også som mennesker, der er det svage led, det er også der har et ansvar for at sikre.

[24:39] Skolelærer: Ja, for at forsøge at forebygge eller forsøge at blive klogere på at være helt sikkert.

[24:46] Martin: Ja, spændende. Ja, vi har i hvert fald ikke flere spørgsmål.

Interview slutter

A.2 Interview - Afdelingsleder, handicapområdet

Interview starter.

00:05 Martin: Jamen vil du ikke starte med at fortælle lidt om dig selv og, hvad du laver til hverdag?

00:09 Afdelingsleder i handicapområdet: Jo. Jeg er afdelingsleder for den beskyttede beskæftigelse i Hjørring Kommune, som er en virksomhed, der beskæftiger førtidspensionister, der har... altså jeg har håndværkere ansat. Så vi er en virksomhed i kommunen. Vi producerer paller og borde og pakker og sådan nogle ting. Ellers er jeg også en del af dagtilbudsområdet for voksne med handicap, sådan helt generelt.

00:49 Martin: Okay. Vil du så ikke starte med at skrive på de to notesblokke her. Vil du ikke starte med på den gule der, når vi siger cybersecurity awareness, at skrive tre ting ned du så kommer til at tænke på?

01:06 Afdelingsleder i handicapområdet: Jo

*Afdelingsleder i handicapområdet skriver på post-its

01:19 Martin: Hvad har du skrevet?

01:21 Afdelingsleder i handicapområdet: GDPR. Og så har jeg skrevet tab+L på pc'en og så "Billeder". Jamen det skal gå hurtigt. Og det ved jeg faktisk ikke rigtig om det går ind under det, men det er det her med, at jeg ved, at når jeg går fra min pc så skal jeg lige lukke den for andre.

01:49 Martin: Hvis vi skal snakke sådan lidt overordnet om IT-sikkerhed, hvad er så dit kendskab til det?

02:01 Afdelingsleder i handicapområdet: Nu har jeg været en del af det her med at lave en hjemmeside indenfor mit område og jeg er mest bekendt med GDPR i forhold til det her med billeder, fordi vi har Facebook, vi har hjemmesider, instagram, vi har alt muligt som profilerer os og fortæller om, hvordan er det at være handicappet i Hjørring Kommune og, hvad laver vi rent faktisk. Der er stor forskel på, hvad man laver. Så det her med, at vi ikke må have ansigter på, det er jo det, der nogle gange også gør det menneskeligt, at fortælle om, at det her... eksempelvis på mit område, så er det det her med, det er mennesker med helt særlige behov, der alligevel, selvom vi har sagt de kan ikke være på arbejdsmarkedet, så kan de alligevel findes en plads til i en virksomhed som os. Det vil vi jo gerne vise, at det kan faktisk lade sig gøre og det gør noget, at man ikke må sætte ansigter på. Så det med billederne, det fylder meget i min optik. Vi må tage hænder med, men ikke ansigter, for så skal vi langt tilbage, hvis nu nogle stopper eller, hvis nogle dør og alle de der overvejelser, der har været omkring det. Og så er det også det her med, at så må vi ikke gemme alle navnene i den samme sag. Det er vel en del af journaliseringsdelen, det kan godt være, jeg blander det en lille smule sammen. Når vi laver lister med CPR-numre som vi skal bruge til noget aftjekning så må de ikke ligge sammen og altså, alt det der, som kan komme til at fylde i hverdagen, hvor det ville være nemt, hvis man bare lige kunne... men det kan man så ikke. Altså det er det, der fylder for os. Og så har jeg været ansat rigtig mange forskellige steder i kommunen. Jeg har været i alle forvaltninger, hvor vi bruger forskellige systemer i de forskellige steder i forvaltningerne. Så jeg bliver også optaget af, at da jeg engang for 15 år siden sad ovre i jobcentret, der havde man et system, hvor man rent faktisk havde adgang til andre afdelinger, børne- og familieafdelingen eksempelvis. Selvfølgelig kan man følge mig derinde og se det, og det blev folk også fyret på, hvis de gjorde sådan noget, men der manglede noget dengang som man også selv vidste. Man tænkte,

det er da godt, at man ikke har en sag i familieafdelingen, altså fordi der faktisk var ret mange, der havde adgang. Men det med systemer og adgange er i hvert også blevet strammet noget op i løbet af de sidste 15 år. Nu bruger man ét system i en forvaltning og et andet system i den her forvaltning og en tredje i, altså.. Så jeg synes, det er vigtigt, men det bliver også lidt tungt. Så for mig er det både det ene og det andet.

05:09 Martin: Ja okay, så det er til en vis grænse eller hvad? Det skal ikke komme i vejen for de daglige opgaver?

05:15 Afdelingsleder i handicapområdet: Ja. Der er jo aldrig nogen, der har sagt, hvis man sidder som en ganske almindelig beskæftigelsesmedarbejder ovre på jobcentret, at man har sagt ja til, at man kan komme ind i en børne-familie sag eller en handicapsag heroppe. Det er der jo aldrig nogen, der har sagt ja til, altså medmindre det har været i en bestemt henseende. Det er på sin plads, at sådan noget bliver skilt ad fuldstændig. Det skal man ikke kunne. Billeder - når en fyr ovre ved mig har sagt ja til og er henrykt over at få sit billede på vores Facebook-gruppe og elsker det, så er det jo lidt ærgerligt, at jeg har lyst til at sige njaaaeej altså vi skal i hvert fald ikke have billeder på, fordi så hvis du ombestemmer dig i morgen, så skal vi igennem hele vores.... Så bliver man lidt begrænset. Men vi gør det så i nogle sammenhænge.

06:12 Martin: Ja, må man ikke godt det, hvis der gives tilladelse til det?

06:14 Afdelingsleder i handicapområdet: Jojo, men problemet er, at det bliver virkelig vanskeligt for os. Jeg har 60 medarbejdere plus mine håndværkere - 103 medarbejdere. Hvis de så stopper ved mig, der er nogle, der holder og starter, holder og starter, så hvornår er det nu han startede og hvor langt skal vi så tilbage i Facebook-tråden for at se om han har billeder her og kan vi så lave en samtykke, der siger du må bruge det når jeg er død. Vi har jo mange, der er meget oppe i alderen også. Så skal vi igennem både dén instagram og dén instagram og dén Facebook-gruppe. Hvor meget skal vi igennem?

06:52 Martin: Så det bliver alt for besværligt?

06:56 Afdelingsleder i handicapområdet: Ja, det bliver alt for... Ja.

07:01 Martin: Når vi så putter det her awareness efter cybersecurity, hvad tænker du så? Er det noget andet, du kommer til at tænke på?

07:13 Afdelingsleder i handicapområdet: Altså, at man er særlig obs på det som udviklingen det byder på. Jeg tænker på, det handler om at udviklingen, den rykker sig hele tiden, så vi skal være sikre på, at når vi introducerer nye systemer eller nye teknikker, eller der kommer et nyt medie, noget vi ikke kan forudsige konsekvenserne af, der skal man være særlig opmærksom på, at.. jeg går ud fra, det er det, jeg ved det ikke. Det er gætværk

07:43 Martin: Der er ikke noget forkert svar. Det er også det, vi prøver at finde ud af.

07:48 Afdelingsleder i handicapområdet: Det er i virkeligheden det, det handler om. At det her, det går hurtigt. Det er superfedt. Der er masser af teknikker, der kommer til at hjælpe os både i pleje og administrativt. Men hvad gør det ved os både i relationerne, hvis vi begynder at bruge teknikker i forskellige robotter, hvad gør det så med relationsarbejdet og så er der hele den administrative del, hvad gør det ved mig, hvad efterlader det af spor på mig, når jeg forsvinder ud af den her kommune, ud af det her liv eller hvad vi forsvinder ud af.

08:25 Martin: Er det en ting, du tænker bevidst over eller er det mere ubevidst i din hverdag?

08:29 Afdelingsleder i handicapområdet: I hverdagen tænker jeg ikke ret meget over det. Jo, på helt lavpraktisk niveau, tænker jeg over det. ugh, jeg er begyndt at afvise cookies, fordi jeg tænker sådan, det skal man nok. Man gør det sådan lidt hovedløst, indtil jeg fandt ud af, jeg får det samme ind på mine medier. Men jeg gør det lidt hovedløst. Desværre.

09:02 Martin: Når du tænker over det, er det så fordi det er træls eller det bliver en ting, der er i vejen for det du skal? Er det mest der, du tænker over det?

09:25 Afdelingsleder i handicapområdet: Det er mest der, hvor jeg opdager, at jeg ikke har tænkt mig om. Altså cookies, og så opdager jeg pludselig, at nu føler jeg mig lidt indskrænket fordi, at jeg har sagt ja til cookies på lige præcis det her område. Det er mere det. Så bliver jeg lidt forskrækket over, kunne du måske have sat dig lidt mere ind i det. Og hvad så når du får en ny telefon, så accepter, accepter, accepter. Det tænker jeg over. jeg tænker også over, at der kommer mere og mere frem på min telefon som jeg har talt om, som jeg ikke har søgt på. Det bliver jeg faktisk lidt forskrækket over. Og hvad jeg ellers har haft af oplevelser. Jeg har talt om på min GPS, at vi skulle på McDonalds og så styrer min GPS mig på McDonalds i Østrig.

10:19 Martin: Det er også lidt skræmmende

10:19 Afdelingsleder i handicapområdet: Det er skræmmende. Vi sidder som familie og egentlig bare skal køre hjem. Skal vi køre forbi McDonalds og så styrer den af motorvej og det hele, og vi har kun talt om det. Det er vildt.

10:35 Martin: Det er også lidt spændende. Jeg læste en artikel fra en forsker, der mener vi lever i en ny tid i kapitalisme, hvor det er data, der er værdi.

10:59 Afdelingsleder i handicapområdet: Ja, du kommer til at kunne styre verden på data.

11:01 Martin: Ja. Og det er lidt skræmmende, som du siger, at vi ikke tænker over det. Vi siger bare ja.

11:37 Afdelingsleder i handicapområdet: Men jeg synes, det er mega spændende fordi at ting kan blive besværlige, men jeg er også bange for, at det der awareness kommer til at begrænse os i udviklingen

11:54 Martin: Hvordan?

11:54 Afdelingsleder i handicapområdet: Altså jeg bruger ikke TikTok, vi må ikke bruge TikTok. De unge mennesker de bruger TikTok alle sammen, tænker jeg umiddelbart. Og de har haft en kæmpe succes. Og Kina kan så overvåge gennem TikTok og det må vi ikke. Men det kunne også være, at TikTok gør noget rigtig godt. Og så begrænser vi, fordi vi bliver bange. Det kan også godt ske i noget større, hvor vi bliver bange. Så vi bliver lidt handlingslammede ind i teknikken måske, og udviklingen den vej, fordi vi bliver bange for overvågningen og en hel masse ting. Så jeg synes, der er mange ting i det.

12:56 Martin: Ja, så man skal heller ikke lade sikkerhedsdelen være begrænsende for, hvis vi snakker arbejdsmæssigt.

13:05 Afdelingsleder i handicapområdet: Nej.

13:14 Martin: Føler du, at det er begrænsende nu for dit arbejde?

13:21 Afdelingsleder i handicapområdet: Nej, men jeg synes, det giver noget pangel. Det bliver

sådan lidt tungt, nogen gange. Men det er fordi, jeg forstår godt, hvorfor vi skal bruge det. Når jeg så skal videreformidle til min personalegruppe, hovedsageligt håndværkere over 50. Når jeg skal formidle de her ting så bliver det lidt tungt.

13:51 Martin: Hvordan gør du det? Træningsprogrammer eller?

13:57 Afdelingsleder i handicapområdet: Nej, jeg giver dem de små tips. Jeg gør det nemt, i skal huske det, det og det, så jeg tager dem i små punkter ud fra, hvad jeg piller ud, hvad de skal være opmærksomme på. Og så har jeg nogle skønne, særligt mænd, der altid godt kan få en god diskussion ud af det her også.

14:46 Martin: Synes du så, det fylder for meget i din hverdag?

14:49 Afdelingsleder i handicapområdet: Nej, det fylder ikke så meget. Det fylder i perioder, som for eksempel når jeg har sat hjemmesiden op og sådan, så fylder det i en lang periode. Så skal der sorteres i nogle billeder og så skal man tænke på det med samtykke. Når det så er færdigt, så kører der en procedure for det. Men det kan godt være, vi mangler sådan nogle awareness programmer som man lige kunne køre igennem. På vores onboarding plan for eksempel. Husk lige, vær opmærksom på. Ligesom man gør med tavshedspligten.

15:54 Heine: Noget man ser meget, det er forbud mod angreb. Der er forskellige angreb såsom phishing og social engineering, hvor de prøver at få noget information til at få adgang til sensitive data. Det er meget den traditionelle måde at se cybersecurity og cybersecurity awareness. Er det noget du ser i din hverdag?

16:34 Afdelingsleder i handicapområdet: Ja. Jeg er også kommet til at klikke ind på en og først da de beder en om et eller andet, altså de giver sig ud for noget andet end de er, og så ryger den hurtigt videre til IT, så skal de jo håndtere det. Men ja, dem får jeg.

16:52 Heine: Når du nu nævner IT, så ses det ofte, at sikkerhed bliver lagt over på IT-afdelingen, men i mange tilfælde er det noget man skal samarbejde om, fordi man kun er så stærk som ens svageste led. Er det noget du lægger mærke til, at du føler et form for ansvar for sikkerheden?

17:33 Afdelingsleder i handicapområdet: Det er det vi gør. Jeg opfatter mig som forholdsvist kvik, så når jeg får sådan en så sender jeg den til IT, fordi det regner jeg med at mine kolleger også gør, så hvis der er et mønster, så samler de det og sender ud, hvis vi skal være opmærksomme på det. Det er dem der har den der sammenhængskraft for alle os, der er ansat i kommunen.

18:03 Heine: Men du kan også godt mærke, du selv har et ansvar?

18:05 Afdelingsleder i handicapområdet: Absolut. Altså jeg har haft ringet ind til IT og fortalt at jeg synes at jeg fik mange henvendelser fra ukrainske kvinder, der elskede mig. Og det er ikke fordi jeg har søgt på noget porno fra Ukraine. Det fik jeg i et årstid. Og det var min arbejdscomputer. Jeg har ikke andet.

19:00 Dylan: Hvor meget omgang har, altså dine medarbejdere med IT? Det er meget analoge ting i arbejder med, i forhold til de her værksteder, så er det noget, der fylder i deres hverdag?

19:27 Afdelingsleder i handicapområdet: Altså mine 103 medarbejdere som er dem der er førtidspensionister har ikke en kommunal pc eller noget. Mit personale de har selvfølgelig. De fører også fakturering og følgesedler og sådan noget, og samarbejde på kryds og tværs, så det fylder da også i deres hverdag. Men det er faktisk ikke noget vi drøfter. Vi kunne godt bruge mere tid på det.

20:09 Martin: Du snakkede før omkring det der med om der var nogen, der så anderledes på det her cybersecurity. Føler du, at der er mange forskellige forståelser af cybersecurity og cybersecurity awareness?

20:30 Afdelingsleder i handicapområdet: Jeg synes faktisk ikke, vi snakker om det.

20:49 Heine: Det kunne jo være en sjov måde at snakke om det, med de ukrainske kvinder, hvis man skulle tage det op og gøre det lidt humoristisk

20:58 Afdelingsleder i handicapområdet: Altså sådan en historie har jeg fortalt fordi den er skideskæg, men det er ikke sådan at vi på ledermøder for eksempel lige drøfter er vi udfordret på noget sikkerhedsmæssigt. Det gør vi ikke. Så er det noget, der kommer oppe fra. I skal være opmærksomme på et eller andet, eller fra IT. Så er det noget vi skal forholde os til og så gør vi så det. Men det er ikke sådan at vi har jævnlige møder om vi overholder det ene og det andet. Min tætteste samarbejdspartner i mit ledelsesteam, vi arbejder tæt sammen fordi vi også er på samme matrice, vi skal også være nogenlunde enige om, hvad vi gør.

22:09 Dylan: Du skrev det her ned med at låse computeren. Hvad er udfordringen ved det? Er det noget i glemmer?

22:18 Afdelingsleder i handicapområdet: Ja. Nu har jeg jo været i alle forvaltninger. Det er i alle forvaltninger.

22:31 Martin: Tror du så, det er fordi man glemmer det eller fordi man tænker, det ikke er så vigtigt?

22:32 Afdelingsleder i handicapområdet: Det tænker jeg, at de tænker, at det først er vigtigt når jeg begynder at skrive ud, at det giver kage på deres regning. Vi havde sådan nogle kurser, hvor jeg tog den der genvej med mig. Der drillede man hinanden på kryds og tværs med det.

23:14 Heine: Er det så noget i er begyndt at stoppe med efter i begyndte at stoppe med at snakke om det?

23:17 Afdelingsleder i handicapområdet: Jeg tænker ikke, at hvis jeg spurgte i mit ledelsesteam, så kender de ikke den der (hentyder til tab+L), og jeg har heller ikke sagt, at vi skal huske det.

23:41 Heine: Det der med, at du har en kontinuerlig samtale om det, det kan bare være kort, så lægger det i baghovedet.

23:53 Afdelingsleder i handicapområdet: Og så deler man også noget viden. Det har du ret i.

24:04 Dylan: I forhold til adgang til systemer. Er det noget du tænker over? Er du blevet overrasket over, at du havde adgang til noget som du måske ikke burde have adgang til?

24:19 Afdelingsleder i handicapområdet: I forhold til hvordan det var engang, så nej. Så er der virkelig strammet op. Alle var jo i det samme system. Så hed det sig også, at vi er en forvaltning, men det er vi ikke. Ikke på den måde. Jeg synes, at der er lukket af og man kan spores.

24:54 Dylan: Ja, for man har jo hørt om sager i Danmark, hvor man har udnyttet sin adgang.

25:06 Afdelingsleder i handicapområdet: Ja, da jeg sad på jobcentret, der ved jeg, at der var nogen, der kom til at søge på eksmanden og røg ud ret hurtigt.

25:35 Dylan: Så man er meget obs på sikkerheden?

25:35 Afdelingsleder i handicapområdet: Det er jo fordi eksmanden finder ud af, hvorfor har hun den her information om mig i en eller anden familieret eller at det er søsterens eksmand og de sidder ovre i familieretten. Det er der man opdager det.

25:54 Heine: Det er den potentielle fare ved at lade en pc stå ulåst, for så er det lige pludselig en anden bruger der kan gå ind og så har man ingen idé om, hvem det er.

26:04 Afdelingsleder i handicapområdet: Jamen det er rigtigt, og jeg kan blive fyret på, at jeg har ladet den stå åben. Jeg skal have det L med.

26:22 Heine: Det er også meget unikt, det der med, hvor langt en ondsindet aktør kan nå med de forskellige brugere. Og om man ved hvor meget man i så fald risikerer at miste

27:01 Afdelingsleder i handicapområdet: Ja. For jeg har jo ikke været udforskende på, hvor langt jeg kan gå ind i vores system, for eksempel. For jeg bruger jo kun det, jeg har behov for. Jeg ved ikke hvad man i så fald ville have adgang til. Det ved min chef måske.

27:30 Dylan: Det er jo også lidt om, hvor ligger ansvaret i forhold til det. Det er jo ikke din skyld, at du har adgang til et system du ikke skal have adgang til, hvis ikke du er klar over det.

27:43 Afdelingsleder i handicapområdet: Nej. Og sådan en som mig er jo lidt farlig i og med, jeg har været i alle forvaltninger gennem 25 år, så jeg har haft adgang til alle systemer. Så jeg ville potentiel have adgang til mange systemer. Men man kan jo sige, at når jeg har en medarbejder, der stopper så er det min pligt, at får dem logget af, så man må gå ud fra mine ledere også har gjort det.

28:52 Heine: Er der noget sensitiv data i arbejder med? Ved du hvordan det håndteres?

29:06 Afdelingsleder i handicapområdet: Ligeså snart der CPR-numre og adresser, så hvis det skal sendes ud af kommunen, så sender jeg det herop og så sender de det ud af kommunen som sikker post. Jeg vil have at det er en anden der gør det med sikker post

29:32 Martin: Hvorfor? Bliver du usikker på det?

29:42 Afdelingsleder i handicapområdet: Det er fordi jeg er usikker på om jeg har tilladelsen til det og hvis den så kommer frem

29:49 Martin: Okay, så det er ikke fordi du er usikker på om det er sikkert, men mere på om det kommer frem?

29:48 Afdelingsleder i handicapområdet: Ja. Jeg har tillid til det. Jeg har bare prøvet, at det ikke kom frem med sikker post. Det der deles internt, deles i et internt system. Så journaliserer man i det interne system. Mine medarbejdere kan godt have adgang til hvad bostøtten arbejder med. Det er som regel ikke relevant, men de har adgange ind i handicapforvaltningen, som de ikke skal bruge til ret meget.

31:20 Dylan: Er det fordi der er cases, hvor det kan være relevant at der er et samarbejde?

31:28 Afdelingsleder i handicapområdet: Ja. De plejer tit at ringe, men de kan bruge systemet også til at informere og varsle. Så der har man jo adgang ind i noget. Så der er nogle systemer der

32:19 Martin: Her til sidst tænkte vi, at den anden blok skulle bruges på at skrive tre ting igen ovenpå den snak vi har haft. Det må godt være de samme ting, men tre ting du tænker på nu, efter

vores snak

*Der skrives

33:19 Afdelingsleder i handicapområdet: Jeg har skrevet at til næste afdelingsmøde vil jeg tage det op med at dele erfaringer og så give eksemplet med genvejen og de ukrainske kvinder. Og så have det som et punkt man drøfter måske hver anden gang. Og så har jeg skrevet at jeg vil følge op på mine adgange i systemerne. Og så er jeg kommet til at tænke på, at vi fik nogle multiple choice programmer, der lærte os om IT sikkerhed. Det kunne mine medarbejdere have godt af. Det var nemt og overskueligt.

34:31 Dylan: Sådan noget, hvad skal man gøre hvis man får en mail og...?

34:33 Afdelingsleder i handicapområdet: Ja, du få den der hurtige e-learning

34:45 Martin: Får du noget træning nu?

34:54 Afdelingsleder i handicapområdet: Nej, jeg fik kun det der dengang.

Interview slutter.

A.3 Interview - Demenskonsulent

Interview starter.

[00:00] Heine: Super.

[00:02] Heine: Og så kommer det til at være cirka en halv tid.

[00:04] Martin: Ja.

[00:06] Martin: Vi tænker, at det bare bliver sådan...

[00:08] Martin: Vi har skrevet nogle ordne spørgsmål ned, men vi tænker, at det bare bliver...

[00:12] Martin: Så hvis der er et eller andet, du tænker over i løbet af, så endelig bare fyr løs.

[00:16] Demenskonsulent: Godt. Ja.

[00:18] Martin: Vil du ikke starte med at fortælle lidt om dig selv, og hvad du laver?

[00:22] Demenskonsulent: Jamen, jeg hedder (Demenskonsulent. red.), og jeg er demenskonsulent på alle ældrecenterne i kommunen. Så derfor er jeg selvfølgelig også lidt spændt på, hvad det er, hvorfor jeg lige blev spurgt. Altså ja, fordi det havde jeg tid til, og det kunne være spændende at finde ud af, hvad det var for noget. Men altså, så det er jeg sådan lidt... Hvad skal man sige? Når jeg lige tænker det der med cyber-awareness og pas på, hvad for noget data... Jeg tænker, det er sådan noget, det dækker over, hvad der er for noget data, man deler i forhold til borgerne. Fordi vi jo nogle gange sidder med noget meget personfølsomt, ikke? Så hvad sender vi? Hvorhen? Og hvornår er det sikkert, og hvornår er det ikke sikkert? Er det sikkert at sende internt i kommunen, eller er det sikkert at sende noget data med noget? Fordi jeg sidder f.eks. med udredninger i forhold til demenssygdomme, så jeg skal nogle gange sende noget til lægen, hvor der er CPR-nummer på, og dele noget med ældre psykiatrien og sådan noget. Så det er sådan lidt der, hvor jeg tænker, jeg måske kommer i kontakt med det.

[01:23] Martin: Vil du ikke starte med, så i forlængelse af det, at skrive tre ting, når du hører begrebet Cyber Security Awareness?

[01:31] Demenskonsulent: Ja.

[01:32] Martin: Tre ord, eller tre ting, du må bare komme til at tænke på.

[01:35] Demenskonsulent: Det første, det er, at jeg tænker, at være sikker at mail, og dele personlige oplysninger. Og så tænker jeg også det der, når jeg får noget ind i min inbox, hvad jeg siger jeg til? Hvad hedder det? Skal jeg bare skrive det, som jeg har samtidigt tænkt på? Hvad accepterer jeg i min inbox?

[02:17] Martin: Ja.

[02:22] Martin: Når vi så siger det her, så er det Cyber Security Awareness. Hvad tænker du så?

[02:28] Demenskonsulent: Det er meget af de tre ting, jeg lige tænker, ja. Den sidste ved jeg, at man klikker på, og når man går ind og søger på et eller andet på sin arbejdscomputer, eller hvad er det for nogle links, man klikker på, og hvad skal man acceptere, og hvad skal man ikke acceptere? Det er det, jeg tænker, at man skal være opmærksom på, for awareness må være at

være opmærksom på noget.

[03:02] Martin: Er det noget, du tænker over i din hverdag?

[03:04] Demenskonsulent: Det er noget, jeg får videre af mine børn, jeg skal. Altså, nogen siger bare, bare tryk OK til det hele, ikke også, og andre de siger, pas lige på. Hvad er det, du trykker på, og klikker på, og hvis det er noget, du er usikker på og sådan noget, så ja. Jeg får jo nogle gange nogle mails om, at på min arbejdsmail, du har ikke hentet den og den pakke, eller du har vundet et eller andet, hvor jeg tænker, det skal jeg i hvert fald ikke lige klikke på, fordi det er helt sikkert, for jeg har ikke bestilt nogen pakke over mit arbejdsmail, så det er i hvert fald ikke noget, jeg lige...

[03:33] Martin: Er det noget, du sådan...

[03:34] Demenskonsulent: Det sætter jeg i spam, ikke også, eller sletter jeg.

[03:37] Martin: Er det fordi, at du har været med i sådan et træningsprogram, eller er det bare sådan en sund fornuft?

[03:43] Demenskonsulent: Det er bare en sund fornuft, jeg tænker, at over min arbejdsmail, der har jeg ikke bestilt noget, og hvis jeg bestiller noget over min privat mail, så ved jeg jo, hvad det er, jeg har bestilt, og hvornår det kommer. Så hvis ikke jeg har bestilt noget inden for de sidste par dage, så vil jeg ikke gå ud og kende noget.

[03:55] Martin: Så det lyder som om, at du tænker lidt bevidst over...

[04:01] Demenskonsulent: Ja, i hvert fald sådan være lidt opmærksom på, hvad det lige er, man klikker på. Fordi man ved jo godt, at hver klik, det efterlader et eller andet spor af et eller andet sted.

[04:12] Martin: Ja.

[04:13] Demenskonsulent: Vi ikke kender de spor, men det har jeg da hørt.

[04:20] Martin: Vi har sådan en spørgsmål, der hedder, hvad tror du, det betyder at være aware i forhold til cybersecurity?

[04:27] Demenskonsulent: Det tror jeg meget, det er det der med at være opmærksom på, hvad det er, man går ud til at kende.

[04:31] Martin: Ja.

[04:32] Demenskonsulent: Ja. Ja, at være opmærksom på det her.

[04:36] Martin: Så det er de ting, der kommer ind hos dig?

[04:39] Demenskonsulent: Ja, og det man selv opsøger selvfølgelig også jo. Men meget af det, der kommer ind, sådan... Hvem er det, der har sendt den?

[04:50] Heine: Ja, det er sådan en mental checkliste, ikke?

[04:51] Demenskonsulent: Ja, og vi har jo det der for eksempel... Hvis nu, hvis jeg sender en mail ud af kommunen, eller for eksempel til ældre psykiatrien, kunne det være, ikke? Det er jo rigtigt. Så får jeg jo sådan en, du vil sende mail ud af systemet, ud af vores organisation, ikke? Og så kan jeg sådan, okay, det er det rigtige sted, jeg sender den hen. Så det er vel også det, der er været

opmærksom på, hvor man sender tingene hen, ja.

[05:12] Heine: Er det noget, du har fået træning i?

[05:14] Demenskonsulent: Nej, men vi har jo fået nogle mails, så nogle gange i forhold til, at nu skal I lige være opmærksom på, at der er noget i omløb, og I skal passe på, hvad I klikker på, og sådan noget. Så vi tager træning som sådan, men det, der blevet at gøre, er opmærksom på, at det er noget, vi ikke bare skal gøre, ja.

[05:30] Heine: Ja, så det er ikke noget, du sådan ser lidt forbi, men det er faktisk noget, du sådan aktivt tænker over og husker på.

[05:35] Demenskonsulent: Ja, ja, ja, ja. Vi får jo lige den der lille reminder, du vil sende mail ud af organisationen. Ja. Og det var faktisk i forbindelse med det første, med det sikre mail der. Jeg gik faktisk med en tanke om, at man aldrig måtte sende fx personnummer, men det må man så godt have internt i kommunen, fordi det er sikre mail.

[05:54] Dylan: Okay.

[05:55] Martin: Ja.

[05:56] Heine: Okay.

[05:57] Demenskonsulent: Det var jeg så ikke klar over.

[05:58] Martin: Hvordan fik du det at vide?

[05:59] Demenskonsulent: Det var fordi, jeg... Det kan jeg jo ikke sende for der er personnummer-pærenummer på. Jamen, det må jeg faktisk godt, når det er inde. Jeg kan ikke huske, hvem det var, om det var TV-stationen eller et eller andet, ja. Hvor jeg fik at vide, det må jeg faktisk godt, fordi internt i organisationen, der er det sikkert. Jeg skal bare passe på, når I sender ud.

[06:18] Martin: Okay.

[06:19] Martin: Har du nogle fornemmelser af, om din kollega, om der er andre forståelser af det at være bevidst eller det at, så skal jeg sige, at have en sikker adfærd eller...

[06:30] Demenskonsulent: Det ved jeg faktisk ikke, fordi jeg har ikke nogle umiddelbare kollegaer sådan lige.

[06:33] Heine: Nej, okay.

[06:34] Demenskonsulent: Nej. Det er samarbejdspartnere. Men de vil jo også få den der, hvis de sender ud af kommunen fx, ikke? Og de får jo også de sammen, så pas nu lige på mig helt.

[06:46] Heine: Er det mere, hvis nu, altså, har du kunne se, altså, at det er måske ikke noget, I snakker om til dagligt?

[06:51] Demenskonsulent: Nej, egentlig ikke, nej.

[06:52] Heine: Noget, der ikke ikke kan blive opundret.

[06:53] Demenskonsulent: Nej, det er ikke sådan noget, der fylder meget i hvert fald.

[06:57] Heine: Det er jo, hvis der var lidt dialogne, så kunne det godt være, at du havde en indsigt

til, om nogen lignende. Ja, så samarbejdspartnere, der måske havde en anden tilgang end du havde.

[07:04] Heine: Eller nogle andre tanker om det.

[07:11] Demenskonsulent: Jo, jeg ved faktisk, der var noget, der skulle sendes. Ja, det var noget, det var også noget, det mindste udredning, som skulle sendes til en. Tænker, fordi noget af det, der var lavet i vores journalsystem, det kunne de godt sende over journalsystemet, men de fysiske test kunne man så ikke scanne ind og så sende. Meget upraktisk. Og så simpelthen, der kan vi sende til mailen til sekretæren. Og så skriver sekretæren tilbage, nej, det kan I så ikke, fordi vores mail er ikke sikker. Nå, nej. Nå, men så må jeg nok putte den ind i kuvert og så gå ned og aflevere den. Det er noget forskelligt faktisk, hvad der er og hvad der ikke er.

[07:46] Martin: Er det noget, der sådan oplever, at det fylder meget i din hverdag? Eller for meget eller for lidt?

[07:52] Demenskonsulent: Nej, det er ikke noget, der fylder meget meget. Altså, det er mest det der... Altså, jeg kan jo godt skrive nogle oplysninger til en samarbejdspartner uden for eksempel at læse, uden at dele CPR-nummer eller et eller andet. Det kan man jo godt. Fordi jeg kan for eksempel skrive, at det er den, der bor på det og det center, ikke? Så er det jo kun dem, der har adgang til det center, der ved dem, der bor derpå. Så det er jo ikke følsomme oplysninger som sådan vel. Så det er jo ikke... Det er jo ikke et del, så det er jo mest det der med CPR-nummerne. Der kommer man lidt ud at flyve, når man er i et system som vores, ikke? Fordi der er så mange, der har adgang til den.

[08:28] Martin: Men når nu I håndterer sådan noget sensitiv information, har I så fået noget... I har ikke fået noget... Jeg tænker noget oplæring eller træning i, hvad man skal gøre med det, hvor man ikke skal...

[08:41] Demenskonsulent: Ikke sådan lige, nej.

[08:43] Martin: Så det er din egen...

[08:45] Demenskonsulent: Det er som, hvad man ellers finder ud af gennem tiden. Ja, der skal man ikke sende hen, og der kan man godt sende hen, og ja, så må man jo så spørge et eller andet sted.

[08:54] Heine: Er det med nogle af skrækscenarierne, som man ser, du ved, med DSP og 7-Eleven for eksempel, er det også noget, du tænker over?

[09:01] Demenskonsulent: Nej, fordi jeg kendte ikke engang de skrækscenarier. Ja, nej, det tror jeg ikke, nej.

[09:07] Martin: Hvor vigtigt, synes du så, at sådan noget er cybersikkerhed, og er det noget, du sådan... Jeg synes, det er bare lidt... Det er faktisk bare lidt sådan benspænd i hverdagen.

[09:19] Demenskonsulent: Nej, jeg synes ikke, det er benspænd som sådan. Jeg ved det faktisk ikke, fordi... Det er jo ikke noget, jeg kan tænke over i hverdagen, men det kan jo godt være det, fordi det bliver sådan en naturlig del af det. Det ved jeg ikke.

[09:31] Martin: Fordi det er bare, hvad skal man sige... Det er bare sådan en ubevidst...

[09:36] Demenskonsulent: Ja, ja, ja.

[09:38] Martin: ... i hovedet, når man tænker over, at det skal man ikke gøre.

[09:40] Demenskonsulent: Det er nærmest så... Ja, det tror jeg faktisk, det bliver sådan lidt... At så hører man måske nogle historier om, at det er gået galt for nogen, fordi de har fået klikket på et eller andet forkert link eller sådan noget, ikke? Ja. Og så tænker man, at det skal man nok lige lade være med. Ja.

[09:52] Martin: Ja.

[09:53] Demenskonsulent: Ja. Men det er jo ikke sådan noget, altså. Det er bare det der cyber-awareness, det var jeg ikke engang klar over, at det var et begreb, tænke der. Okay, hold da.

[10:01] Heine: Ja, det handler jo meget om det med, hvordan skal man sige, at du kommer ind, og så... Altså, at du skal bruge den her sunde fornuft. Det kan godt være, at man så ser en masse skrækscenarier, men så skal man ikke være bange for stadig at bruge de redskaber, man har til rådighed, så længe man bare har en sund fornuft bag. Som du selv nævner med, at du tjekker, hvem sætter han af fra, og tjekker indholdet, og sørger for ikke at klikke på de forskellige links, og ikke lukker ind på forskellige hjemmesider. Så kan det jo også være...

[10:30] Demenskonsulent: I hvert fald være opmærksom på hvilke hjemmesider, ikke også, om det er... Ja, eller at man...

[10:35] Martin: Der er også en svær balance i det der med, at du skal også kunne udføre dit arbejde, og være i kontakt med hvem, du nu skal.

[10:42] Demenskonsulent: Ja. Det er jo så heldigvis ikke i IT, der er så stor en del af mit. Men alligevel har vi jo meget digitalt, ikke?

[10:49] Martin: Ja.

[10:50] Demenskonsulent: Ja.

[10:51] Dylan: Har I ikke nogle systemer fælles, altså? Nu ser du, at I har meget kontakt med læger.

[10:55] Demenskonsulent: Ja, ældre psykiatri og sådan.

[10:58] Dylan: Og vel også de centrer, som det gælder på. Der er ikke nogen fælles systemer eller noget. I bruger det alt.

[11:05] Demenskonsulent: Altså, der er journalsystemerne til ældre sentrerne. Der er journalsystemer, vi kommunikerer igennem.

[11:12] Dylan: Er der noget... Nu tænker jeg bare sådan... Det er jo mange brikker, der ligesom skal spille sammen. Og hvis I har noget fælles sted at have de her ting, hvis mange ting er over mail, så kan man også tænke, at der er mange ting, der kan gå galt. Altså sådan... Som du siger med at sende ting måske lige i stedet hen. Er det noget, der er frustrerende? Er der nogen ting, som du vil ønske var nemmere i jeres arbejde, sådan kommunikationsmæssigt?

[11:36] Demenskonsulent: Altså, jeg synes jo, det kunne være dejligt, hvis vi kunne kommunikere alt. Til for eksempel lægerne og ældre psykiatrien. Hvis alt det foregik over journalsystemet. Fordi så vidste vi jo, ligesom det var samlet et sted. Ja. Og så tænker jeg, der er nogen her inde i det her hus, der har styr på, hvordan det fungerer. Så jeg kan være helt trygt på, at her kan du skrive lidt. Naturligvis biviste om, at der kan komme noget på, og at der kan komme nogen, der skal have

adgang til det. Så man skal selvfølgelig også være opmærksom på, hvad man skriver. Men at du ligesom kan dele ting. Og adgang til de samme informationer for eksempel. I stedet for, fordi ældre psykiatrien for eksempel ikke har adgang til vores journalsystem. Så det bliver jo sådan lidt dobbelt arbejdet. Der er mange ting, I skal gøre flere gange.

[12:18] Dylan: Det er det frustrerende.

[12:20] Demenskonsulent: Ja, men også bare lige den der lille ting. Med udredninger er jeg godt... Når jeg udfylder selve udredningen inde i vores journalsystem, den kan jeg godt vedhæfte en mail inde i journalsystemet til lægen. Men selve den fysiske test, som borgeren har lavet, hvor der er noget med at skrive nogle sætninger og efterligne nogle figurer og sådan noget, lave en urskive og sådan, den skal jeg simpelthen ned med. Ind og så vedhæfte. Altså bare lige sådan en ting, hvor jeg tænker, det må der være nogen, der kan finde ud af at lave.

[12:50] Martin: Hvorfor kan det ikke lade sig gøre?

[12:52] Demenskonsulent: Hvorfor skal man lave dobbelt arbejde? Og det er så ikke engang sådan, fordi det mærkelige det er jo så, jeg kan godt til selve udredningen, der kan jeg godt vedhæfte de fysiske tests som fil. Men når jeg så sender den videre, så følger det ikke med det der vedhæftet.

[13:10] Martin: Mærkeligt. Men jeg tror du så, at du ville være mere trygt måske, hvis du vidste, at I havde måske et fælles system, der var krypteret. Så man vidste, at det var sikkert. Vil du være mere tryg ved det end at skulle for eksempel sende mails?

[13:31] Demenskonsulent: Helt sikkert, fordi som jeg sagde, så ved jeg jo, at der er nogle andre, der har et arbejde omkring at passe på det. Ja, det er sikkert. Så det ville jeg helst sikkert være.

[13:41] Heine: Men tror du godt, at du selv kunne være mål for et angreb, hvis de få adgang i dine login-oplysninger for eksempel?

[13:49] Demenskonsulent: Ja, vi har jo for eksempel fået at vide, at vi må ikke gemme koder på vores arbejds-PC. For eksempel koden til vores journal, den må vi ikke have lov til at gemme. Netop fordi, hvis der så er nogen, der kommer ind, så har de jo adgang til alle de oplysninger, jeg også har adgang til. Og det er jo allerede derinde. Jeg har for eksempel ikke adgang til borgere, der ikke er flyttet ind på ældrecenter. Så der er det jo allerede delt ind. Så bare da de kommer ind, så kan de jo se alle oplysningerne på de borgere. Så tager man dem, så ved de jo nogle ting der om dem. Og har man det CPR-nummer, så kan du jo gøre rigtig meget.

[14:24] Heine: Så det er jo der, hvor de ondsindede aktører, de kan komme ind?

[14:28] Demenskonsulent: Ja, ja. Og det er i hvert fald noget, vi har fået at vide, at vi må ikke gemme koder. Det gjorde jeg også før i tiden, så fik jeg at vide, at det måtte jeg ikke.

[14:36] Martin: I har jo ikke noget sådan en træning i cyber-sikkerhed?

[14:40] Demenskonsulent: Nej, nej, nej. Så det er sådan mere en mail, der lige kommer ud om, at det passer lige på, at der er noget i opløbet.

[14:46] Martin: Ja.

[14:47] Demenskonsulent: Ja, så der, ja. Lad være med at klikke på og sådan noget der.

[14:50] Heine: Og det synes du er nok til at ligesom nok at forberede dig i forhold til det arbejde, du

laver?

[14:56] Demenskonsulent: Hvis det værste sker, så er det jo ikke.

[14:59] Heine: Nej, nej.

[15:00] Demenskonsulent: Nej, så er det jo ikke.

[15:01] Heine: Det, jeg plejer at sige, det er jo, at det er ikke, hvis du bliver hacket, men når du bliver hacket.

[15:06] Demenskonsulent: Ja, ja, ja.

[15:07] Heine: Og hvor man kun er så sikker som ens svageste led. Og hvis man sådan har det lidt i mente, så kan man tænke, ja, er det så egentlig nok at sætte en mail ud i forhold til at skulle have den her viden? Fordi den er måske, den er ret central i forhold til at kunne oprette sikkerheden og arbejdsdagen.

[15:22] Martin: Ja, det er også lidt det, der er sådan, hvad skal man sige, i fundamentet. Det her begreb, det her med cybersecurity bevidsthed eller awareness, systemerne egentlig er ret gode til at f.eks. at opfange sådan nogle mails med spam i og sådan noget. Men er det så menneskeligt, eller også der bliver det svage lød, fordi vi kan komme til at klikke på den her link eller sådan noget? Men det er kun sådan, hvad skal man sige?

[15:49] Demenskonsulent: Men vi bliver ikke oplæret i det. Det var jo helt tilfældigt det der. Jeg tror faktisk, det var fordi, der var et eller andet, jeg var inde her ved IT. Og så, hov, du har altså gemt din kode, det må du jo ikke. Nå, men så skal jeg jo sidde og huske det hver eneste gang, og når man så skifter sig i det måde, hvad man var nu lige, det var altså noget ikke. Så er det meget lettere, at den lige er gemt. Og det må du altså ikke. Nå, okay. Det var jeg jo ikke klar over. Hvis ikke jeg havde været herinde, så kunne der jo endelig være nogen, der havde snubbet. Og du skal jo bare... Fordi jeg får jo de der SMS'er engang imellem om, at du har ikke hentet, eller du har ikke... Den pris, du har vundet i et eller andet i Lottisystem, den har du ikke afhentet. Den SMS kan jeg godt få, ikke? Og hvis de har adgang til min telefon, kan de jo også meget nemt få adgang til, fordi der er min kalender faktisk også på. Så har de jo nemt adgang til min kalender om dermed mange andre ting, ikke? Hvis jeg for eksempel sagde, nå, det var da mærkeligt, jeg har ikke det. Jeg må heller lige skynde dig at klikke, hvis det er, at du ikke vil have den sendt tilbage, eller hvad nu de skriver, ikke?

[16:44] Martin: Ja.

[16:45] Heine: Så du kan jo godt se fidusen lidt i nogle af de ting, faktisk?

[16:48] Demenskonsulent: Ja. Og så tænker man, hvor i verden har de fået mit telefonnummer fra? Er det tilfældigt, de bare skriver, ikke? Og jeg er jo mega nervøs, hvad det angår, så jeg har jo ingen idé om, hvordan tingene foregår, sådan teknisk.

[17:03] Heine: Nej?

[17:04] Demenskonsulent: Nej.

[17:05] Heine: Men det er også det, der er lidt... Det er lidt, hvordan skal jeg sige, spøjse paradoksale ved awareness, fordi så længe du ved, hvad du ikke skal gøre, og hvad du skal gøre, så behøver du egentlig ikke at vide noget som helst om det tekniske, for at være sikker.

[17:19] Demenskonsulent: Nej, og man er jo aldrig sikker.

[17:20] Heine: Nej.

[17:25] Martin: Det er jo det, der er lidt... Ja, jeg ved ikke, sådan en barriere for, at du kan føle, at du kan gøre dit arbejde, og bliver du sådan lidt...

[17:36] Demenskonsulent: Nej, det er ikke en barriere. Jeg er bare opmærksom på det. Bare opmærksom på det også, fordi vi får at vide det der med.

[17:44] Martin: Så det er ikke noget, der hindrer noget?

[17:45] Demenskonsulent: Nej, det er det ikke. Altså, det er jo kun det der, hvor det bliver irriterende, når man skal til at lave dobbelt arbejde, ikke? Men ja, det er ikke sådan noget der.

[17:54] Dylan: Så det her med dit login og sådan noget, er det, at I skulle skifte det hver 6. måned?

[18:01] Demenskonsulent: Ja, jeg mener, det hver 6. måned. Så kommer der sådan en advarsel et par dage før, at nu den bliver udløbt.

[18:07] Dylan: Skal I bruge det meget i dine hverdager?

[18:10] Demenskonsulent: Det skal jeg jo hver eneste gang.

[18:11] Dylan: Hvad eneste gang du gør noget?

[18:13] Demenskonsulent: Hver gang. Når jeg åbner min computer, jeg har en fastnets-computer, og så har jeg en tablet, og så har jeg en telefon.

[18:21] Dylan: Ja.

[18:22] Demenskonsulent: Ja, min telefon den har bare en kode. Men for eksempel tablet, hvis jeg skal gå ind på vores journalsystem, så skal jeg jo hver gang logge ud, hvis jeg skal logge ind på en nyt center, og der er jo så tretten i kommunen. Og der skal jo være, jeg tror, det er 10 bogstaver, og det er to eller tre tal, ikke også? Og det må ikke være én, du har brugt inden for de sidste 3 år eller sådan et eller andet, hvor man sådan tænker, at det er der, hvor jeg bliver nødt til at have en lille seddel i min telefon. Og så kan jeg ikke huske det for gang i gang, hvor jeg nu er kommet til i min...

[18:52] Dylan: Har I sådan noget med... du får ikke sådan nogle mobilkoder, sådan noget tofaktor, som du skal?

[18:58] Demenskonsulent: Øh, ikke ret tit. Jeg har brugt det, men jeg kan ikke lige huske, hvad det er i hvilken samling. Jeg har fået det, men det er ikke sådan noget til hver gang, jeg logger ind.

[19:06] Dylan: Nej, okay.

[19:07] Demenskonsulent: Nej. Men det er jo så den login, jeg ikke må gemme på computeren. Ja.

[19:12] Dylan: Ja.

[19:13] Martin: Du har ikke sådan en password manager?

[19:19] Demenskonsulent: Nej, nej, aldrig. Og det er faktisk også koden, der skal også være et stort bogstav.

[19:27] Dylan: Ja, det er lidt urimeligt, at du skal huske det hele, men du må ikke skrive det ned andre steder.

[19:31] Demenskonsulent: Jo, det må jeg godt rent fysisk, men jeg må ikke skrive det ned ellers, nej. Det er i hvert fald en fordel ikke at være arbejdsgiver. Men jeg ved for eksempel, det er egentlig, jeg deler kontor med. Hun har 32 eller 36 cifre, hun skal trykke på sin computer for overhovedet at komme ind. Så siger jeg, jeg tror ikke, du skal gå op til IT-afdelingen. Der må være et eller andet på din computer, der gør det, for det skal jeg altså ikke. Ja, hvor jeg tænker, hun sidder over det papir hver morgen. Eller så kan hun ikke komme ind overhovedet og åbne computeren for at skrive sit password.

[20:05] Heine: Okay.

[20:06] Demenskonsulent: Ja.

[20:07] Martin: Hvad laver hun?

[20:08] Demenskonsulent: Hun er supervisor.

[20:10] Martin: Okay.

[20:11] Demenskonsulent: Også på ældrecentrene, ja. Så det er ikke fordi, vi har noget meget sådan top secret informationer, ja. Men nej, ja. Hold da op.

[20:21] Martin: Ja.

[20:22] Demenskonsulent: Jeg synes også, det er meget.

[20:25] Heine: Fordi der findes nemlig de her password-managers, så har du det, der hedder Master Password. Og så kan du logge ind, og så genererer den forskellige passwords til de forskellige ting, og så kan du bare copy-paste det direkte faktisk.

[20:37] Demenskonsulent: Ja, det tror jeg faktisk, jeg har på min egen computer. Der er i hvert fald nogle gange, at hvis der er nogle forskellige sider, jeg sådan jævnligt logger ind på, hvor der skal passwords på eller sådan et eller andet, jamen så tager det gennem nok.

[20:53] Martin: Paradoksalt nok, på mit arbejde, der blev, vi havde også en password-manager. Dem der laver den, de blev så hacket.

[21:00] Demenskonsulent: Ja. Men det igen, ingen er jo sikker i det her.

[21:05] Heine: Nej.

[21:06] Demenskonsulent: Og jeg kan da godt tænke, de der cyber-pirater, hvorfor synes de måske, at jeg kunne være interessant?

[21:17] Dylan: Ja.

[21:18] Demenskonsulent: Altså, ja.

[21:19] Martin: Ja.

[21:20] Dylan: Det er jo nok ikke dig som privatperson, men du har adgang til utrymme.

[21:24] Demenskonsulent: Ja, ja, ja, jamen det har jeg jo, ja.

[21:26] Dylan: Tænkte du nogle gange over, hvis nu er dit login blevet stjålet, hvor meget skade, man ville kunne gøre med det? Altså, ved du hvor langt du kunne gå i system? Altså, hvor meget data du kan få adgang til?

[21:41] Demenskonsulent: Ja, hvad kan man få adgang til? Ja, altså jeg kommer jo aldrig længere faktisk ind til borgernes informationer. Jeg har ikke adgang til noget sådan her, hvad vil jeg, kontoer her i kommunen for eksempel. Ja, der kunne tømmes eller et eller andet.

[21:57] Dylan: Men der er jo meget sådan medicinale informationer og journaler. Det er jo ret vigtigt.

[22:03] Demenskonsulent: Ja, det er der.

[22:04] Dylan: Det er jo lidt uhyggeligt, hvor meget man vil kunne.

[22:09] Demenskonsulent: Ja, og der kan jo også stå et eller andet. Der kan også være en lille huskeseddel versionalsystem på en eller anden borger, i forhold til hvis de har en mobiltelefon eller de har et hævekort, og de ikke kan huske koden af, hvor det så står. Og så har de adgang til den der journal, så har de også adgang til det der kort faktisk.

[22:28] Heine: Ja, og det er jo sådan noget, man skal skrive bag øret. Det er jo en af de mulige ting, som de kan have adgang til. Så er det det, man lige skal have i mente.

[22:38] Demenskonsulent: Ja, og du kan jo være enig i princippet. Hvis nu jeg har en borgers CPR-nummer, så kan jeg jo egentlig gå ned og hæve nummer 10, for eksempel. Ja. Hvis man havde brug for at få fat i sådan noget. Ja, det er også lidt. Men det er ikke sådan noget, der fylder 90% af min arbejdstid.

[22:57] Martin: Nej, det er mest fordi, det her er det, du har snakket om. Det er mest bare sådan ubevidst.

[23:02] Demenskonsulent: Ja.

[23:03] Martin: Så det er ikke noget, du bevidst tænker over. Nu skal jeg gøre det her, fordi...

[23:07] Demenskonsulent: Nej, det tror jeg, det er nok noget, man har lært sig bare, at det er sådan det er.

[23:11] Heine: Har du kun mærkt forskel på din arbejdsgang i forhold til Cyber Security, når den kommer til før og efter corona?

[23:18] Dylan: Så er der mere digitalt arbejde og...

[23:21] Demenskonsulent: Nej, jeg vil sige... Nej, ikke sådan det der awareness, men... Jeg vil sige, min IT-kundskaber, de er blevet bedre, fordi vi er begyndt at lave møder online. Ja, der var jo rigtig lidt. Der, hvor jeg altid tog min taske og bilen, og ellers så kører det ud, ikke også? Der er det lige pludselig, så er det blevet mere... Det er blevet tryggere,i hvertfald, og ikke så grænse-overskridende, at man skal sidde foran en skærm og have møde med mange mennesker og sådan noget. Ja. Altså, det er ikke sådan... Måske ikke det der cyber awareness, men mere det der med kundskaberne. Ja.

[23:52] Martin: Havde du hørt om cyber security awareness før?

[23:55] Demenskonsulent: Jeg havde faktisk ikke rigtig hørt det. Jeg kunne gætte mig til, hvad det sådan cirka var.

[23:59] Martin: Ja.

[24:00] Demenskonsulent: Og hende, der spurgte mig, så sagde jeg, kunne det være sådan noget i den her retning, at de spørger mig om sådan noget, at det ved jeg ikke en pind om, siger hun så, men... Jamen, det prøver vi.

[24:11] Martin: Sådan.

[24:12] Demenskonsulent: Ja. Men jeg er jo nok heller ikke den typiske målgruppe, I lige tænker på umiddelbart sådan.

[24:17] Heine: Ja, men det sjove ved dig, det er, at du har nogle helt andre ideer og indsigter, end hvad vi selv har, for eksempel.

[24:25] Demenskonsulent: Okay, ja.

[24:26] Dylan: Vi har også IT til en ekstremt stor del af vores verden, ofte langt dybere end det, men det er jo din hverdag, der er mest repræsentativt måske for størstedelen af medarbejdere i kommunen også.

[24:41] Demenskonsulent: Ja, det tror jeg.

[24:42] Dylan: Så det er jo ingen indsigter at have.

[24:43] Demenskonsulent: Altså, alle medarbejdere, du går rundt med en tablet, den er jo næsten lige ved at vokse ud i armen, ikke? Ja, fordi alt er der på, ikke? Og når vi får den der ugenlige mail om, at nu er journalsystemet nede, det er bare en nedtur, for så har man ikke adgang til noget som helst. Heller ikke medicin, for eksempel. Ja.

[25:01] Dylan: Er det så helt analogt, eller stopper man bare hele tiden?

[25:04] Demenskonsulent: Der får de bare ingen medicin. Så tager man det lidt på hverdag i Æsken og siger, det er fornuftigt ud, det her, ikke? Ja, det her, ikke? Og for det meste er det heller ikke så lang tid. Det er jo mere det, vi ikke kan logge ind. Så I er meget afhængige af systemerne? Ja, det er vi jo. Det er man jo i hele hverdagen. Vi ligger jo bare ikke mærke til det mere, vel? Altså, det er jo lidt ligesom det der med, at ... Altså, vi ved jo også godt, og det er bare blevet sådan en del af ens hverdag, hvor man tænkte, hold da op, da man bliver mærksom på det, og så sidder og siger et eller andet med ... Det kunne være spændende at tage til Holland, ikke også? Woopsie, tænk så næste gang, jeg åbner for eksempel Facebook eller sådan, og så er der rigtig mange Hollands rejse tilbud, ikke også? Hvor man tænker, det var der mærkeligt, jeg har ikke been at søge på noget, ikke? Ja, helt tilfældigt, ikke også? Men det er jo bare blevet, vi har blevet accepteret det. Det er hverdagen nu.

[26:00] Martin: Men det er også derfor, at det er super spændende at snakke med dig. Fordi vi kan jo godt have en anden forståelse af, Martin: hvordan IT-sikkerhed skal være, eller hvordan systemerne skal være.

[26:10] Demenskonsulent: Men jeg hører jo også til den generation, der ikke er overvokset, altså jeres generation, og dem, der kommer efter. De er jo opvokset, men det er bare en naturlig del, er det ikke? Ja. Mit barnebarn her var jo ikke mere end tre før, da han vidste, hvordan han lå sin forældre. Telefoner op og sådan noget, de er jo næsten født med telefonen i hånden i dag, eller bl.a. eller andet, ikke? Så der er måske der, man skal sætte mere ind, fordi vi, ja, det ved jeg ikke.

[26:39] Dylan: Man kan jo heller ikke glemme, altså, ja, man kan jo godt lave en masse IT-systemer til de nye unge, der kommer, men der er jo stadig mange, der stadig også arbejder, og samfundet skal jo stadig også passe på de mennesker, der ikke er vokset op med. Så det er jo lidt en svær, ja, det kan jo heller ikke blive for digitalt.

[26:58] Demenskonsulent: Nej, men det er jo faktisk det, altså, Hjørring Kommune, de siger jo, at de er en digital kommune. Så det er jo det, man lægger op til. Det er jo det de fleste kommuner, at det skal være. Så lidt papir som muligt. Og alligevel så printe vi ud som, jeg ved ikke hvad. Fordi der er bare det der med, når man har det ved siden af to forskellige ender, og det er sådan, der er forskellen, ikke?

[27:20] Dylan: Er der noget i arbejdet, der går ud fra det ofteste af ældre med demens, hvor hele IT-delen er forvirrende også? Har de noget interaktion?

[27:32] Demenskonsulent: Ja. Det kan i hvert fald være nogle af de første tegn på en demenssygdom. Det der med, nu kan de simpelthen ikke forstå. Altså, den her fjernbetjening er også. Hallo? De tror, det er telefonen. Eller de kan ikke finde ud af, at det der fjernbetjening, det fungerer ikke. Altså, hvad er det for en knap, man skal have? Så kan man sætte nok så meget omkring den røde knap, det er den, du tænder og slukker på og alt sådan noget. TV-programmerne, der bliver to dage efter, de lige barnebarnet har været, sat det i system, så virker det ikke igen og sådan noget. Det er typisk der, hvor man kan opdage, at der er et eller andet, der er skredet. Der er andet, som ikke fungerer mere. Det er typisk med sådan noget IT. Eller de tekniske ting, kaffemaskinen eller vaskemaskinen.

[28:15] Dylan: Ja, for det ligger ikke på deres ryggrad, de er jo vokset op med.

[28:18] Demenskonsulent: Ja, det er jo, fordi det er jo nye ting. Og det er også der, hvor vi ser, at nogle gange nogen flytter ind på et ældrecenter, de har en mobiltelefon, og det fungerer rigtig fint, og lige pludselig kan de ikke finde ud af det. De kan ikke finde ud af, hvordan telefonen, selvom de måske har haft den der telefon i 10 år, og det er den samme telefon og alt sådan noget, men de kan ikke finde ud af det. Dylan: Det er vildt skræmmende. Ja, så er det jo lidt, ja, ja, ja. Fordi det er jo hele frontalnettet, der går ned, og også hukommelsen. Og vi har faktisk en del borgere, der kommer ind, der har arbejdet inden for, nej, det er ikke for at skræmme jer, men har arbejdet inden for IT, men starter med at få en sygemelding på stress, fordi de ikke kan finde ud af arbejdet. Det bliver for uoverskueligt, ikke også, eller skal lave arbejdstidsplaner, eller et eller andet, hvor de begynder at tage det med hjem, fordi de ikke kan nå det på arbejde, og det hele bliver sådan lille og uoverskueligt, fordi man ikke har de der evner mere. De smuldrer, ja.

[29:29] Martin: Og stress, det er sådan...

[29:33] Demenskonsulent: Det kunne godt være, altså, vi har delt og flyttet ind, hvor at stress har været den første diagnose, de har fået. Stress eller depression.

[29:43] Dylan: Men det er ikke fordi, at stressen, hvor du sagde, at demens, men fordi de bliver stresset, er deres...

[29:48] Demenskonsulent: Nej, det er fordi symptomerne kan være de samme. De tidlige symptomer på den, man synes om, kan være de samme. Og man kan jo nogle gange sige, at når de får diagnosen, så kan familien sige, okay, faktisk allerede for 10 år siden, der var jo lige den der ferie, hvor at vi ikke kunne finde ud af at komme hjem, eller et eller andet, eller... Ja, der var noget, man ikke kunne finde ud af, eller ikke dobede op, eller ikke huske, hvad dag det var, eller et eller andet, ja.

[30:13] Martin: Hvor tidlig kan man få af det, eller se det?

[30:19] Demenskonsulent: Det er meget... Ej, jeg vil sige, de yngste, de har været sidst i 40'erne. Det er meget ungt. Typisk er det plus 60, plus 65.

[30:29] Heine: Så er det lige en 10-20 år mere.

[30:33] Demenskonsulent: Men det er nogle andre borgere, vi får ind nu, end vi gjorde for 10 år siden, for eksempel. Det er nogle borgere i nogle høje profil jobs, der har haft et jobliv, der har været presset og belastet.

[30:50] Dylan: Så de har altså næsten brændt hjernen.

[30:53] Demenskonsulent: Ja, ja, ja.

[30:55] Dylan: Så man skal passe på sig selv?

[30:57] Demenskonsulent: Det skal man. Sørg for at få koblet af. Det gør jeg i hvert fald. Når jeg er fri halv fire, så slukker jeg min arbejdstelefonen. Tænder den igen næste morgen. Men jeg får tit mails fra afdelingslæder kl. kvart i 11, hvor jeg sådan tænker så godt over i seng. Men jeg læser den ikke før næste morgen.

[31:14] Dylan: Nej.

[31:15] Martin: Nej.

[31:16] Demenskonsulent: Men ja.

[31:17] Heine: Smart.

[31:18] Demenskonsulent: Det er en meget skræmmende sygdom.

[31:19] Martin: Det er virkelig... Når jeg er hjemme hos mine forældre, deres nabo er også en ældre kvinde. Og hun... Ja, jeg er sikker på, at hun også er det mænd, der begynder at være. Det er godt nok... Også fordi hun har boet her i lang tid, så har jeg snakket lidt med hende. Det er godt nok skræmmende, synes jeg.

[31:37] Demenskonsulent: Ja. Og det kan jo være sådan nogle tekniske ting. Det kan også være sådan noget som bilen, for eksempel.

[31:41] Martin: Ja.

[31:42] Demenskonsulent: Hvordan var det nu, at du lige skulle tænde lyset? Ja, alle sådan nogle ting. Der er mange ting. Tak. Skal I bruge den her til noget, eller skal jeg bare smide den ud?

[31:51] Martin: Vi skal tage lige en sidste ting faktisk.

[31:52] Demenskonsulent: Okay, ja.

[31:53] Martin: Ja, nu har vi jo startet med de der tre ord der, og ting du... Vil du så ikke slutte af med at skrive på den blå der? Tre ting... Det ved jeg ikke. Det kan godt være det samme, : men der er bare tre ting, du tænker over nu, efter vi har snakket.

[32:07] Demenskonsulent: Ja.

[32:08] Martin: Hvis der er nogle nye ting, du... Eller et eller andet, vi har nævnt, eller... Det må også godt være det samme, hvis... Et eller andet fra samtalen, du tænker. Det her, det var da... Det var da spændende. Det kan være, at jeg tænker over det endnu mere fremover.

[32:28] Demenskonsulent: Ja, hvad hedder så noget? Jeg skriver lige sikkert mail igen, men det er det, der er med, men...

[32:33] Dylan: Man kan finde ud af, om manøvre rundt i sin mail

[32:37] Demenskonsulent: Ja, på... På samarbejdspartere også, det var lige. Og det kunne faktisk også godt være... Det der med, at journalsystemet taler sammen. Det må I gerne bringe videre, hvis det er.

[33:02] Dylan: Ja, jeg synes, det er interessant, at... Man opdager mange... Altså... Mange sjove ting. Mange finurlige ting, hvor man tænker, hvorfor er det ikke anderledes.

[33:10] Demenskonsulent: Hvor mange forskellige har I egentlig haft inde? Er det okay, hvis jeg bare lige skriver sådan her?

[33:14] Martin: Ja.

[33:15] Demenskonsulent: De hænger lidt sammen, kan jeg se.

[33:17] Martin: Ja.

[33:18] Heine: Ja.

[33:19] Dylan: Du har 2 ud af 5 vi skal snakke med.

[33:21] Demenskonsulent: Men hvor mange forskellige fælter arbejder I indenfor?

[33:23] Martin: Ja, vi er inde for biblioteket. Og så tror jeg, vi har lidt...

[33:29] Dylan: Ja, der er også noget for noget skole.

[33:31] Martin: Ja, skole.

[33:32] Dylan: Skole har vi senere på Hjørring Skolen.

[33:33] Demenskonsulent: Så jeg er måske den eneste fra ældrecentret.

[33:35] Heine: Det tror jeg faktisk, det er.

[33:36] Martin: Ja. Altså, vi sagde i hvert fald, at vi gerne ville snakke med så mange forskellige som muligt.

[33:40] Demenskonsulent: Ja, ja, ja.

[33:41] Martin: Så vi kunne høre lidt forskellige ting der.

[33:43] Demenskonsulent: Spændende.

[33:44] Martin: Ja.

[33:45] Demenskonsulent: Det er spændende at se, om I kan se noget forskel i forhold til, hvad vi arbejder med.

Interview slutter.

A.4 Interview - Bibliotekar

Interview starter.

00:12 Heine: Vil du starte med at fortælle lidt om dig selv og hvad du laver til dagligt?

00:15 Bibliotekar: Jamen, det kan jeg da godt. Jeg hedder Bibliotekar (anonymiseret) og jeg er ansat ved Hjørring Bibliotekterne min arbejdstitel hedder Digital Bibliotekar, og det er ligesom mange af mine arbejdsopgaver. Jeg sidder med den digitale bagside af biblioteket, vores hjemmeside, vores digitale ressourcer, databaser, sådan håndtering af det, sociale medier, og så har jeg også noget front arbejde, altså hvor man møder publikum. Så det er sådan den korte version kan man sige.

00:43 Heine: Okay, så det vi vil gøre i dag er at, vi gerne vil have fokus på begrebet Cybersecurity Awareness, og så forstå din forståelse af det. Det er ikke så meget om dine kapabiliteter eller hvad du, altså hvor god du er til det er vi ikke interesseret i. Det er mere din forståelse af begrebet og det er lidt det som er formålet med vores, hvad kan man sige, undersøgelse og vores problemformulering på specialet her. Øhm, så det er lidt det vi kommer til at snakke om. Først nu er der lige et par post-its der, hvis du vil skrive på den gule, tre ord ned når du hører ordet Cybersecurity, de første tre ord som falder dig ind.

01:21 Bibliotekar: Ja det kan jeg godt, bare sådan, ja det prøver jeg at gøre.

01:43 Heine: Ja, hvad har du skrevet?

01:44 Bibliotekar: Jeg har skrevet GDPR, Keylogging og hacking, og det er sådan noget som er. Det er ligesom tre begreber som er taget ud af min virkelighed, min arbejdsvirkelighed kan man sige. 01:57 Heine: Hvorfor lige de tre begreber? Hvorfor ikke phishing eller ja nogle af de mange andre typiske (begreber), e-læringsværktøjer for eksempel. Undervisning.

02:09 Bibliotekar: Ja, hvis vi tager dem en ad gangen, GDPR det er bare sådan noget jeg kan mærke, jeg har været i biblioteksbranchen i nogle år og det er bare sådan noget, hvor der bare er blevet skruet på en knap, hvor man lige pludselig er kommet i tanker om, hov det kan måske være vi sidder, altså vi er bare et bibliotek, men vi har måske adgang til nogle systemer, noget data som er følsom for nogen, det er sådan den ene del af det, det er noget jeg kan mærke er blevet eskaleret. Og så keylogging, det er fordi der har været i vores branche nogle mega uheldige sager lige nøjagtigt med det, det er sådan noget vi har brugt mange timer over at tænke på hvordan man håndterer sådan noget, på en meget lavpraktisk måde som også kan fungere i hverdagen. Og så hacking det er fordi jeg sidder med hjemmesider, sociale medier og sådan noget, og det er bare, det er sådan noget jeg tænker på en gang imellem. Og hvor der også, jeg sidder med i sådan nogle nationale netværk, hvor man kan se kolleger i andre kommuner, hvor de bare sådan mister det hele, så ja.

03:16 Heine: Hvad så i forhold til dit kendskab til cybersecurity, hvad kan man sige, hvor stor er din viden indenfor området?

03:24 Bibliotekar: Medium til OK vil jeg sige, det er sådan lidt svært at sætte en eller anden, hvad kan man sige, 0 til 100 på ikke altså, jeg bilder mig ind at jeg synes jeg har rimelig styr på sikkerhed et eller andet sted, men så er det også en cybersecurity, når I siger det kunne man måske også, det er så der jeg tænker, hvordan definerer vi det, altså fordi det er bare så mega bred en paraply at det er jo alt muligt. Det er jo sådan noget som det her, men det er også alt muligt andet, så det

jo i hvert fald i min optik. Så jeg tror og håber at jeg har sådan en rimelig god forståelse af det, men som man så også kan se og som der har været ufatteligt mange eksempler på efterhånden synes jeg, det er at når man ligesom tænker der er styr på det her pis, det er der bare ikke. Det er jo en kontinuerlig proces, så det er jo ikke sådan et mål kan man sige.

04:16 Heine: Når du siger det er bredt, vil du prøve måske at sætte lidt ord på hvad for nogle ting du tænker når det er sådan et paraplybegreb? Hvad for nogle underemner mener du der er i Cybersecurity og måske også i Awareness delen af feltet og emnet? 04:30 Bibliotekar: Jamen jeg tror, jeg mener faktisk lidt det som jeg, det man kan sige med processen, at man ikke er færdig, man kan ligesom godt tænke at vi er dækket af, at vi sådan har brandsikret eller prøvet sådan at fremtidssikre os lidt mod et eller andet, men der er jo bare, der sidder bare nogle kloge mennesker et eller andet sted med nogle rimelig trælse hensigter også, som nok skal komme videre end det. Så derfor skal vi også bevæge os hele tiden, altså og så kan man sige, hvad er det? Og det ved vi måske ikke fordi den ikke er bygget endnu. Giver det mening?

05:00 Martin: Der er ikke noget sådan end goal, man bliver aldrig færdig, man bliver aldrig sådan nu er du sikret?

05:06 Bibliotekar: Det tror jeg er meget uforsigtigt og påstå at man tænker nu er der styr på det. Der er altid nogen som nok skal komme med et eller andet counter, øh, modoffensiv som tænker, hvordan får vi prikket hul i det, eller nårh de har ikke tænkte på det ovre i hjørnet eller noget i den stil. Men ja, altså jeg tror jeg kan mærke sådan i mit arbejde at det i hvertfald er noget over tid, hvor man bliver mere og mere, ja aware, er jo nok ordet. Altså sådan med hvor meget skal man passe på og hvad er det nu, er det nu en god ide at vi får lavet det her på den måde, eller burde jeg sende den her ting eller sådan noget i den stil. Lige nu er vi for eksempel igang med en migration fra sådan nogle servere og fællesdrev til at flytte det hele over i OneDrive og i den oprydningsproces har vi sådan nogle scanningsværktøjer som IT har til at køre, der sådan lige scanner alt vores mails og dokumenter igennem for lige at få se, har vi noget der ligger som vi måske ikke skal have til at ligge. Altså bare sådan helt basic, der er vi helt nede på bunden synes jeg og der vælter jo frem med ting og sager fordi man, fordi der er hverdag og man kan godt gå og tænke, det skal vi også lade være med at gøre og vi skal gøre sådan her. Men det skal også være færdig klokken et i dag, så jeg skynder mig lige og lave et eller andet.

06:26 Martin: Ja det er jo netop også det der bliver en svær balance jo, det jo sådan at man skal være sikker og bevidst omkring, men man skal også kunne udføre et arbejde.

06:37 Bibliotekar: Ja det er lige nøjagtigt det, hvor mødes de to henne. Og det er så procestingen også, de mødes bare ikke det samme sted hele tiden, altså nogengange bliver der skruet mere og mere op for (...)

06:50 Martin: Så det er noget I tænker over, er det noget du kan mærke i hverdagen også blandt dine kolleger måske, er I bevidste omkring cybersecurity eller noget I sådan bevidst snakker om eller?

07:03 Bibliotekar: Mmm, ja, altså hvis man nu tager udgangspunkt i de her ting for eksempel (hans tre punkter), nu tager vi keylogging, altså der har vi haft, der er rigtig mange mennesker som bruger biblioteket som en print central, hvor man går ned og printer fordi det ikke kan betale sig at have en printer derhjemme, men vi har lukket af for alle vores USB porte, fordi det er ligesom den primære adgang til keylogging. Øhm og så bliver man lige pludselig meget bevidst om når folk kommer med deres USB pinde og siger “Kan jeg få det her ud”, nej det kan du ikke. Der bliver det ligesom inkorporeret i en hverdag der fungerer på en eller anden måde, men også tilstedekommer noget

brok og diskussioner, noget med publikumservice, altså det der med, det plejer vi jo at kunne og det kan vi lige pludselig ikke længere, ergo serviceforringelse sådan noget i den stil. Men også sådan noget, det er rimelig paradoxalt, hvis man tager GDPR tingen, vi har i en del år haft et, vi har et fagsystem, et biblioteksfagsystem, når vi slår dig op for eksempel (peger på Heine), så ser vi hvor du bor henne og sådan noget, og vi ser dit CPR nummer og så siger du at du gerne vil bestille Nietzsches samlede værker, et eller andet kommer du og siger, og den har vi ikke selv så jeg sender den lige til en eller anden, og så før i tiden, for uhyggeligt kort tid siden, der ville vi have sendt dit CPR nummer i en mail der ikke er krypteret, ja, men i fagsystemet, altså vi snakker i nyere tid ik, men i fagsystemet har du et eller andet nummer som man ikke kan bruge til en skid overhovedet, som kun duer (virker) inde i vores fagsystem og det er så det jeg skulle sende til nogen, kan du ikke lige reservere til låner osv osv. Men det der personhenførbare data altså at der ligesom er kommet en bevidsthed, som ligesom er blevet inkorporeret i dagligdagen, hvor det så fungerer på en måde, hvor folk egentlig også kan se at det kunne godt være vi lige. . .

08:51 Martin: Så man tænker måske mere over, sådan sensitiv informationer, at man ikke skal. . .

08:55 Bibliotekar: Ja det er primært det vi arbejde med, synes jeg et eller andet sted, at vi sådan skal

09:00 Martin: Så det er ikke så meget med at der er nogen der, det der med beskyttelsen udadtil, men det er mere med at passe på den information man har?

09:07 Bibliotekar: Ja, man kan sige beskyttelsen udadtil, den er todelt hos os, fordi vi har jo ligesom, vi har en IT infrastruktur hos os, men den er ude i en armslængdeprincip fordi at vores infrastruktur, altså i huset, den bliver lavet hernede et eller andet sted, vi bor jo et andet sted, så det er lidt distanceret på en eller anden måde, det er ikke sådan noget vi, det er meget kommunalt ikke, det er noget IT de tager sig af, det fikser de nok, det er sådan den ene del af det. Men så har vi så vores, hvad hedder det, vores fagsystem, vores biblioteksystem, vores hjemmesidedrift og det er ligesom, det kører et andet sted fra, så det er sådan, jeg tror måske nok det måske er en lidt usund tankemæssigt at det er distanceret og ikke er noget vi selv har styr på, men samtidigt med så ved jeg at dem som sidder i den anden ende og tager sig af det, de har markant mere styr på det, altså vi har ikke ressourcer til at have IT personale der kan styre sådan noget, men det gør måske også lidt at sådan tankesætsmæssigt, så er det ikke så present i hverdagen, der er styr på det regner vi med.

10:20 Heine: Kan du så mærke at noget af det her cybersecurity, at det måske bliver en hæmsko engang imellem i forhold til dine daglige arbejdsopgaver? For det er noget som er meget i forhold til det vi har undersøgt, det kan oftest være en frygt for i hvert fald topledelsen, at hvis der kommer for meget cybersecurity ind kontra det man skal beskytte, så er det måske ikke det værd at miste de timer.

10:45 Bibliotekar: Nej jeg tror faktisk lige netop ikke, det kan godt være det er paradoksalt i forhold til mange andre steder, men jeg synes ikke vi har været ude i noget med at det er blevet egentligt mere besværligt, men det er bare sådan noget med at man skal gå fra sådan noget “vi plejer” til nårh nu skal du lige gøre det på den her måde, fordi om jeg skal finde dit CPR nummer inde i vores biblioteksregister eller om jeg skal finde dit lånernummer som det så hedder, sådan et randomt genereret nummer det er samme forskel arbejdsmæssigt, men det er det bare ikke for din datasikkerhed kan man sige. Der har vi været sådan rimelig heldige. Så er der måske noget med for eksempel det der med at vi har lukket af for alle USB porte, en anelse mere besværligt, men når man så snakker med folk om det, og vi fortæller dem det er fordi sådan og sådan, at der er nogen som har mistet jeg ved ikke hvor mange penge og sådan noget fordi de har, fordi de er

blevet keylogget, så er folk jo med på at, altså dialogen, og så kommer der måske et ok resultat ud af det i 90% af tilfældene ik, og så i de sidste der ikke kan få printet et eller andet ud, de finder nok på et eller andet andet.

11:44 Heine: Nu var vores formål lidt om Cybersecurity Awareness, nu har vi snakket meget om Cybersecurity generelt. Nu har vi nævnt det et par gange, når nu vi nævner begrebet Cybersecurity Awareness, hvad er det så du tænker generelt om, når du hører det ord

12:00 Bibliotekar: Vi har snakket lidt om det på vores kontor, for jeg tror at jeg synes det er meget, nu er det også selvfølgelig her, hvor jeres fagterm er et eller andet sted, men som jeg ser det så er det, det der med at man sådan har det ligesom at det ligger underbevidst på en eller anden måde. At man sådan er, at der sådan en, hvad kan man sige, en underliggende tanke om, et eller andet man skal passe på. Det kan både være internt, men det kan også være noget eksternt, men måske også en, det ved jeg ikke, verden er jo et rodet sted pt, at ting er mere sårbare måske, end man sådan lige regner med, og man skal jo ikke bladre i ret mange aviser før man ser nu er det her nede, den her er blevet hacket og sådan noget i den stil. At noget man sådan har tænkt der er meget robust før, det er måske der den ligger i awareness tingen, at der er sådan en instabilitet, skrøbelighed indbygget sådan samfundsmæssigt også lige pludseligt, at man ikke skal regne med noget og SAS går ned eller et eller andet i den stil. Altså der er ikke noget som er sikkert, sådan længere på en eller anden måde. Så derfor får man også lyst til måske at sikre sig så godt som man kan ikke, og ja, giver det mening?

13:13 Heine: Ja, for det er lidt to fænomener som vi også er stødt på, med at, for det første så handler det ikke om hvis du bliver hacket, men mere når du bliver hacket, og at man har den indstilling. Og det andet det er, jamen hvis du har en, kan man se hvorfor de lige præcis vil angribe den branche og hvad for noget data tror du så de vil gå efter, fordi de angriber den branche. Så hvorfor ville de angribe den branche, så hvis de angriber biblioteket i Hjørring, for eksempel, hvad er det så for noget data de kan få ud af det, hvordan vil så kunne være skadelige overfor dem som, overfor jer som organisation, men måske også de mennesker som de prøver og target. I forhold til de mål her, er det måske noget du kan se gennem din generelle arbejdsdag og gennem det her awareness concept. Er det noget du kan se der ligesom er, deres påvirking og influence, hvor målene på angrebene og hvad de ligesom er?

14:09 Bibliotekar: Nej det tror jeg netop ikke jeg kan faktisk, jeg synes det er sådan helt randomt. Hvor man har læst om her for nyligt en eller anden hackergruppe som lægger udenrigsministeriet ned bare for at sige det kan vi. Altså sådan på den måde så bliver det noget, så er det noget magtdemonstration, men selvfølgelig er der også, der er ikke kun magtdemonstration i det, der er også noget med at hvis man kommer ind i nogle systemer og man så har adgang til alt muligt, så kan man sige, vi på biblioteket har nogle personfølsomme oplysninger og vi har noget lånerhistorik faktisk en lille bitte grad. Det har vi så ikke så meget længere, fordi det har vi også fået skåret væk, så jeg kan ikke se hvad du har lånt for tre måneder siden for eksempel noget i den stil.

14:58 Dylan: Det holder man ikke på længere? Man holder ikke så længe på lånerhistorik længere, er det på grund af noget sikkerhed?

15:05 Bibliotekar: Det er sådan en GDPR ting. Paradokset er så at man kan slå det selv, altså hvis du selv bruger vores app for eksempel, så kan du gå ind og sige, prøv lige at gem min historik, så hvis du tænker har jeg læst det her før, et eller andet i den stil, så kan du slå den til fremadrettet.

15:23 Martin: Hvordan kan det være? Er det fordi man ikke må se hvad du har læst?

15:25 Bibliotekar: Hvis nu du havde lånt 300 bøger om at lave bomber for eksempel og så

15:30 Martin: Men det er da meget rart at vide, er det ikke, hvis jeg har det?

15:32 Bibliotekar: Nej, jeg tror faktisk det er meget rart ikke at vide et eller andet sted, det er ligesom der vi sikrer at der ikke er nogen, at man ikke kan føre noget tilbage, det er helt fuldstændigt derfor, man kan ikke knytte dig sammen med. Men jeg kan godt se det i en efterforsknings kontekst ville det måske være meget fint, men...

15:49 Martin: Hvis der var en lånte, ja, 300 bøger om at lave bomber, så kunne det godt være at man lige skulle høre hvorfor?

15:55 Dylan: Det kan jo også udnyttes, hvis nu jeg læser noget politisk som staten ville være imod det jeg læste.

15:59 Bibliotekar: Fuldstændig, for hvor går grænsen ik? Altså man kan sige at bomber er meget håndgribeligt, men hvis du nu bare læser de forkerte bøger på en eller anden måde, hvis du er voldsomt fascineret af en eller anden yderligtgående politiker eller sådan noget og du bare har styr på det hele, du har lånt alt, eller sådan noget i den stil, eller bare sådan noget Mein Kampf, som du har fast udlån på nonstop. Og det er jo også, man kan jo sige, biblioteket er også pakket ind i en ideologisk skal om der skal være fri og lige adgang for alle og der skal ikke være nogen som er mere eller mindre overvåget end andre. Vi leverer det og så er det ligesom den frie tanke der opererer derfra, så det er sådan lidt, hvor godt det passer sammen med sådan en, ja for eksempel en overvågning, efterforsknings kontekst ikke særlig godt kan man sige, men altså det er så ude i en etisk diskussion et eller andet sted.

16:51 Heine: I forhold til awareness konteksten, er det så også noget du tænker over til hverdag, om det sådan er bevidst eller ubevidst?

16:59 Bibliotekar: Altså bare sådan i min helt private hverdag eller?

17:02 Heine: Nej arbejdsdag

17:04 Bibliotekar: Jamen, jeg tror det hænger sammen, det er meget det som jeg har nævnt før, hvor det er sådan blevet automatisk inkorporeret i meget af min hverdag, ja.

17:17 Martin: Tror du der er forskellige, blandt dine kolleger, er der sådan forskellige opfattelser eller forståelser af (Cybersecurity awareness)

17:24 Bibliotekar: Fuldstændig, det helt sikkert.

17:25 Martin: Også i forhold til, nu er det svært at måle graden på hvor bevidst man er om det, men...

17:33 Bibliotekar: Helt lavpraktisk, så har vi jo et biblioteksrum, altså vi har låste døre ind til vores kontorer og sådan noget, det skal man have og vi skal låse vores computere når vi går fra dem, det skal man, det siger Ulla som sidder lige herude. Men det giver også god mening fordi de står åbne med adgang direkte ind til kommunens IT infrastruktur, så hvis man får fat i en af vores computere, og ved hvad man laver, så har man altså adgang til en del. Men sådan noget som det at lige at trykke lås når man går, den er svær. Allerede der bliver det svært. Så kan man sige, det er spændet på awareness-delen, den viser det faktisk meget godt, at der er nogen, jeg er sådan lidt fascistoid omkring det og låser også andres computere, hvis jeg lige kommer forbi en, så siger jeg lige plup og så, men der er også andre som tænker, årh det går nok, jeg skal bare lige herover.

18:26 Martin: Tror du så det er fordi de glemmer det, eller fordi de tænker det ikke er så vigtigt?

18:28 Bibliotekar: Det ved jeg ikke, jeg ved det simpelthen ikke, fordi så skal man til at låse op igen, det er også lidt besværligt og sådan noget i den stil. Lidt besværligt. Men jeg tror faktisk det der med, det er spændet ik, er der forskel på det, ja der er virkelig forskel på det og jeg er også, jeg vil være meget uforsigtig hvis jeg sagde at der ikke bliver sendt nogen som helst emails med CPR numre nede fra os.

18:53 Heine: Det er også et andet fænomen som går ind i, at man kun er så sikker som ens svageste led, og hvis man så ikke ved hvor meget adgang de har, så hvis for eksempel, at du mister, at der er en som får adgang til dine login oplysninger, ved Hjørring Kommune så godt hvad for noget data de kan tilgå, i forhold til jamen hvor meget adgang der er fra din login.

19:17 Bibliotekar: Ja, altså det er jo så heldigvis, kan man sige, begrænset, jeg er faktisk ikke engang selv helt klar over, hvor meget data jeg har adgang til, fordi jeg har ikke undersøgt, lad os se hvor langt vi kan gå ud på drevet, jeg har ikke gået i gang med den øvelse, men jeg går ud fra og håber på at der er nogen nede i IT, som har sat nogle begrænsninger op på mig og på min bruger, på hvor galt det ligesom kan gå.

19:44 Heine: Men det bliver lige pludselig meget katastrofalt på en eller anden måde og meget, hvad kan man sige, ragnarok-agtigt, du ved ikke helt hvor meget data de egentlig kan få adgang til, hvis nu det er din bruger eller hvis det er en kollegas bruger.

19:59 Bibliotekar: Ja, det kan man godt sige på den måde, men det er også en almindelig driftssituation, Martin er ansat på biblioteket, han skal have adgang til de her mapper og han skal have adgang til de her systemer, det synes jeg er en meget logisk måde at lave det på. Det er det samme når jeg sidder og laver hjemmesider og jeg skal give adgang til en af jer, så får du redaktøradgang og så skal jeg nok sørge for at du ikke kan pille inde i coren af et eller andet dopa system eller sådan noget i den stil, det skal jeg nok selv gøre.

20:29 Heine: Så i forhold til det at være aware, i forhold til cybersecurity, vi har nævnt lidt på det, men måske lidt mere konkret, hvad er det så du tænker det indebærer?

20:36 Bibliotekar: Det er et fluffy spørgsmål synes jeg.

20:48 Heine: Ja, det er også tankerne vi skal have igang

20:51 Bibliotekar: Jamen jeg tror, hvis det giver mening for jer, altså awaredelen for mig er, det er sådan en bevidsthed om at man sådan, to ting, at man skal opføre sig ordentligt, passe på og at ting kan gå galt og så de to ting er der selvfølgelig en vekselvirkning, så hvis man ikke gør sit arbejde ordentligt, på en eller anden måde, det tror jeg awaredelen er for mig, man gør det jo ikke for hyggens skyld.

21:21 Martin: Også at være aware over konsekvenserne, hvis man ikke er bevidst om det?

21:25 Bibliotekar: Ja, jeg tror konsekvenserne er svære og overskue, men at der kan være en konsekvens egentlig, på den måde, og at man på den måde egentlig, jeg tænker når, i min hverdag, når man arbejder med nogen systemer, hvor man så har, det er sådan respekt overfor dem som bruger biblioteket på en eller anden måde, at man ligesom opfører sig ordentligt, passer på deres ting ik. Det ville være det samme hvis jeg var en mekaniker og nogen kom og afleverede deres bil, så passer jeg også på den, altså på den måde ikke. At man sådan ligesom, jeg tror det er det, at man sådan er et ordentligt mennesker, hvis man skal op på en eller anden etisk platform, men ja,

det kan man jo også sagtens være uden at være aware kan jeg godt se, men ja, jeg tror det er det, et eller andet sted, at der er en respekt for det man laver og det måske er sådan et middel på en eller anden måde, ikke et mål, aldrig et mål, men et middel til en del af den oplevelse for dem som jeg ligesom skal servicere og det arbejde jeg skal lave, at man er, ja opmærksom.

22:39 Heine: Ja, også i forhold til de her ting, det virker jo ikke til at være mega uoverskueligt at skulle låse sin PC eller at man tager nogle af de her koncepter i brug. Men er det måske noget som topledelsen, nogle af dine chefer, er det noget de kommer ud med og fortæller, okay nu skal I lige huske at låse PCen når I går derfra, er det der beskeden hovedsagligt kommer fra?

23:00 Bibliotekar: Ja det vil det være, altså nede hos os, det er så igen det der med at vi er et led ude, fordi vi er nede på biblioteket og det her er kommunen, men ja det ville det være. Det er jo vores chefer og vi har så også haft Ulla, som I lige har snakket med heroppe også, nede hos os og lige have en gennemgang af hvad er det for nogle scenarier vi kan være ude i og hvordan kan vi meget meget let, helt lavpraktisk komme en god del af det til livs altså, men det der med at få informationer til at sive ud i en hverdag, det er bare, det du kan edermandme skriver mange mails om sådan noget. Et eksempel, jeg laver også grafik og kommunikationsarbejde på biblioteket også, jeg har egentligt mange hatte på, men på et tidspunkt havde jeg lavet sådan en plakat, sådan noget med at man skulle give kage hvis man glemte at låse sin computer og den tænkte vi at vi simpelthen ikke kunne sætte op, fordi så meget kage kan vi slet ikke håndtere. Men altså, det er sådan noget man kan se blive bedre, for når vi så har haft besøg af Ulla for eksempel og det bliver italesat, så har man det måske i en, det er måske ikke det man snakker over hver dag over frokosten, men at det ligesom er, at der er et frø som er sået og så kunne jeg godt, jeg er sådan lidt firkantet, så jeg kunne godt tænke mig at vi siger fra på onsdag låser alle kraftædeme deres computere og låser også andres når de går forbi den, men sådan fungerer virkeligheden bare ikke, det tager tid og gøde den her awareness åbenbart ikke.

24:37 Heine: Mennesker er jo vanedyr kan man sige.

24:41 Bibliotekar: Fuldstændig, men noget som også gøder det er jo for eksempel sådan noget som nyheder, når man så ser at alt muligt bare bliver hacket fra en side af, eller at der har været brud på et eller andet, det ville jeg så også våge at påstå at er med til det implicit. At folk kommer i tanker om, som jeg også nævnte før at verden er bare mere usikker end man måske tror.

25:03 Heine: Ja, man kan sagtens se det i eksemplerne, bare med DSB og 7/11 for ikke så lang tid siden. I forhold til cybersecurity og cybersecurity awareness, hvor vigtigt synes du egentligt det er i forhold til dit arbejde?

25:18 Bibliotekar: Det er top vigtigt synes jeg, ja, helt sikkert, men også fordi vi er sådan et, måske i forhold til andre organisationer, så biblioteket er bare gennemdigitaliseret, altså meget af det vi laver, alle transaktioner, vi har engang imellem, hvor vores biblioteksystem går ned, ikke hacket, men der er nedetid, og når der er det, så går organisationen mere eller mindre i stå, altså man kan godt finde nogle bøger frem manuelt, men du kan ikke låne dem ud, du kan ingenting. Det er bare så meget vores organisation og være digital og der kunne jeg forestille mig at det kunne gå knap så galt hvis man er i en børnehave eller et eller andet i den stil, så ja, det fylder. 26:05 Martin: Ja, det er nærmest kritisk at det virker faktisk 26:10 Bibliotekar: Jamen det er det og samtidigt med at, det hænger også lidt sammen med perifert sammen med jeres opgave, så kan man også, den anden dag for eksempel, i lørdags der havde vi mistet forbindelsen til CPR registeret, som så betyder at vi ikke kan oprette en ny låner for eksempel, fordi vi ikke kan hente info og så er der sådan lidt, hvorfor. Før i tiden ville man bare være inde på en eller anden statusside, der vil være noget nedetid, der er nok nogle teknikere som går og roder med et eller andet. Men nu der er det sådan,

kan man også mærke at det er og det er også en del af awareness-tingen at, hmm, er der sket et eller andet som ikke skulle være sket, og skriver rundt til alle mulige kollegaer i andre kommuner, har I det samme problem, og de har også det samme problem, det er en national ting, der et sket et eller andet og så er der endelig en som finder et eller andet med, hvor der står nårh, forresten vi har noget opdaterings et eller andet.

26:56 Martin: Så man tænker straks, åh nej

26:58 Bibliotekar: Jamen, det tror jeg faktisk at det er noget jeg er begyndt mere med at før havde man bare tænkt, nåh ja, servicevindue eller et eller andet, men selv at sådan nogle kritiske ting, altså forbindelsen på CPR registeret er ret kritisk for os, og for ret mange, og hvis man har lagt det ned, så er der godt nok mange ting der ikke fungerer lige pludselig, og det er også sådan en baglæns awareness-del et eller andet sted, at man, at det er ikke meget sådan noget ulven kommer, men mere at ulven den er her, altså tænker man sådan helt automatisk først, før man...

27:38 Martin: Men det kan jo også være en meget god motivation til at gøre noget

27:42 Bibliotekar: Få det fikset øjeblikkeligt, ja lige præcis.

27:47 Heine: Altså man kan sige i forhold til vigtigheden, hvor alfa omega det er at der er styr på det, det er noget som der er centralt fokus på for jer. I forhold til, hvor meget kender du så til, du har nævnt det lidt i forhold til CPR, men ved du hvordan det bliver sendt, opbevaret og håndteret i din arbejdsgang? Ved du mere eller mindre, hvordan det bliver håndteret?

28:09 Bibliotekar: Altså, hvordan det fungerer i vores fagsystem? Altså det bliver sendt krypteret i hvert fald og vi har det ikke som sådan, vi har sådan et datapoint vi har der ligger et eller andet sted, hvor vores fagsystem kan kigge ned i gennem en sikker forbindelse, det cirka så meget jeg ved om det. Jamen også sådan noget som sendt frem og tilbage, for så er det nemlig den der, vi arbejder i to. Vi har sådan et fagsystem vi arbejder i, men hvis vi skal sende bestillinger til andre biblioteker, så skal man ud af det og så over i et andet krypteret system, men det er så der man har muligheden for at for eksempel sende CPR nummer, det er ikke noget, der er potentielt nogen som kan få fat i det, men det er der, hvor man skal vælge de her lånernumre, men hvordan det bliver sendt og sådan noget, jeg går ud fra at der er styr på sikkerheden, men jeg ved det ikke sådan helt konkret.

29:01 Heine: I forhold til, nu kan du se vigtigheden af din, af Cybersecurity i din hverdag, kan du så også se, lad os nu sige, nu har du selv nævnt det, man tager det altid over til IT afdelingen og så siger de har styr på det. Kan du også mærke at der måske skal være lidt ansvar på jer som også bruger det, i forhold til det ikke kun er den her lukkede afdeling der skal stå for det, men det er måske os alle sammen som skal bidrage til og kunne hjælpe med at forhøje det?

29:28 Bibliotekar: Ja, altså man kan sige, vi har jo ikke dataen som sådan, man kan ikke gå ned og stjæle en computer nede ved os og så har man alle vores låneoplysninger, det kan man ikke, så er det mere den daglige drift, altså håndteringen af det, og det synes jeg er top vigtigt. Så kan man sige at IT afdelingen, det er mere infrastrukturen på en eller anden måde, de har jo ikke håndteringen af dataen som sådan, men det er mere sådan at de har lavet et ordentligt system nede hos os håber jeg. Men jeg har tænker egentligt også på, nej men det er fordi jeg bliver ved med at tænke over det der overvågning og de der bomber, at der er jo også, nede hos os, det er jo så også en anden del, som der er en del der bruger, vi har åbne WIFIs for eksempel nede hos os, som er noget der har været snak om i nogle år, hvorfor har man et åbent WIFI og hvorfor har man det ikke så man skal logge på, så vi kan se hvad du laver. For der har vi nemlig haft nogle

eksempler på at IT afdelingen lige pludselig står der, så der foregår også en eller anden form for overvågning, altså den datatrafikmæssigt, altså hvor de siger, hvem er det der sidder ved computer sådan og sådan, for vi kan se at der sker et eller andet.

30:36 Heine: Det er det samme med fænomenet, med at hvis du har en arbejds pc, så skal du kun have arbejds tingene derpå, så skal du ikke tilgå offentlige netværker. Det er jo i en idealistisk og perfekt verden.

30:50 Bibliotekar: Jo, det har vi også noget med arbejdere i fagsystemer i hvert fald, så skal vi, eller vi kan kun, det kan kun fungere hvis vi kører på en VPN forbindelse og det er et meget fint benspænd og specielt kan man sige, post-corona er der ret meget hjemmearbejde, jeg arbejder enormt meget hjemme, men der er det en god løsning til at man ikke sidder alle mulige steder nede på en eller anden random cafe.

31:20 Heine: Apropos corona, har du kunnet mærke forskel på dit syn af cybersecurity og awareness-delen efter corona?

31:26 Bibliotekar: Det ved jeg ikke, det ved jeg simpelthen ikke, det tror jeg faktisk ikke. Men det er nok fordi jeg sidder på et kontor, som jeg gjorde. Vi havde diskussionen før også, et eller andet sted og der er ikke det eneste, nej det tror jeg faktisk ikke. Altså man kan jo sige at VPN forbindelsestingen er blevet universel i kommunen efter det, men før det der havde jeg bare en anden VPN forbindelse.

31:57 Heine: Okay, så du har ikke kunnet mærke forskel hverken arbejdsgangen, hvad med angreb, altså der har ikke været så stor forskel på før og efter corona?

32:05 Bibliotekar: Ikke noget jeg har tænkt over i hvert fald.

32:10 Heine: I forhold til din arbejdsdag, du har måske nævnt det lidt, men jeg tænker det er okay lige at få det genopfrisket, hvilke dele kommer cybersecurity og awarenessdelen til syne generelt?

32:21 Bibliotekar: Altså helt lavpraktisk i min arbejdsdag, lige om lidt når jeg er færdig med at snakke med jer, så skal jeg jo ned og passe biblioteket altså ude i udlån, og der er det en del af det, for der står man jo med, inde i systemet, men ude i et offentligt rum. Det er sådan noget, det tænker jeg i hvert fald over, når man arbejder med det også, vi har en meget meget åbent bibliotek, vi har nede hos os, folk kan kigge med sådan inde over skulderen og sådan noget, ja også sådan noget med, hvad man sender til folk. For der bliver bare sendt utroligt meget mellem biblioteker, vi har sådan noget interubant samarbejde og hvad der bliver sendt der, det er især der hvor vi passer på synes jeg.

33:06 Heine: Ja, så til sidst, vil du skrive tre ting ned som du kan tage med fra det her interview, som du måske kommer til at tænke lidt mere over og det må du gerne skrive på den blå.

33:20 Bibliotekar: Det kan være jeg kommer til at skrive det samme.

33:35 Heine: Det helt fint, alt data er valid data.

33:53 Bibliotekar: Skal jeg læse det op også?

33:54 Heine: Ja, meget gerne.

33:55 Bibliotekar: Der er to af dem, der er sådan en jeg har skrevet lokal forankring, men det er faktisk det der, det kan jeg godt se at, det der med ansvarsdelen, hvor ligger ansvaret henne, fordi

det er super let bare at sige at IT tager sig af det, at det er deres problem, men måske er det også ens eget problem, eller det er det jo. Og den hænger lidt sammen, nu har jeg skrevet PC lås, jeg tror måske vi skal have en lille kampagnetur nede hos os, det kan godt være jeg skal have kageplakaten op alligevel. Nu er der så mange som låser deres computere at vi ikke kommer til at drunker fuldstændig i kage. Og så den der GDPR ting, jeg har skrevet GDPR igen fordi det er sådan en, den er bare altså det er der, hvor vi sådan kan behandle data ordentligt, på en eller anden måde, det er der, hvor vi virkelig har sådan, altså hvordan de bliver håndteret og hvordan de bliver sendt rundt.

Interview slutter.

A.5 Interview - Medarbejder 1 i databeskyttelse

Interview starter

[00:00] Medarbejder i databeskyttelsesteamet: Hvad kan jeg svare på og spørgsmål for jer?

[00:02] Dylan: Ja, det ville vi høre fra dig var også lidt.

[00:06] Dylan: Nu hørte vi jo fra nogle af de andre, at der kommer det her cyber security awareness primært.

[00:14] Dylan: Altså generelt tendens fra deres private liv.

[00:19] Dylan: Hvor man hører om de her gls-beskeder eller postnord beskeder og sådan noget.

[00:26] Dylan: Når du sidder i sådan en stilling, hvad betyder det så i din hverdag, det her cyber security?

[00:34] Dylan: Du tænker selvfølgelig over det, men i din arbejdsgang kommer det så til syne der?

[00:40] Medarbejder i databeskyttelsesteamet: Altså man bliver utrolig paranoid, når man arbejder med databeskyttelse. Lige meget i hvilken grad det er. Jeg har meget opmærksom på, hvad er det vi sender ud af huset, og hvordan sender vi det ud af huset? Hvad er det vi sender afsted, hvor meget har man behov for at få, og hvor meget er rart at få? Der er en kæmpe forskel på need to og nice to. Og det er nok den største barriere. Det er, at folk i det kommunale ofte har været i det kommunale længe, eller i hvert fald i det offentlige. Så de har måske adgang til lidt for mange systemer, eller de har været vant til, at jeg kan bare gå hen og spørge Hanne, og så kan hun lige hente tingene til mig, og så sender man frem og tilbage. Sådan nogle ting lægger jeg meget mærke til, når man snakker med folk, og de så stiller spørgsmål, eller hvorfor kan jeg ikke længere åbne det og det fagsystem, eller hvorfor har jeg kun en kigge adgang, i stedet for en administrator adgang osv. Så på den måde er det noget, jeg ser meget. Så er jeg lidt mere paranoid, når det kommer til hjemmet. Jeg har da selvfølgelig en iPhone, det skal man jo have skulle jeg til at sige. Man skal jo have en smartphone, men vi har ikke hverken en Google Hub eller en Alexa, eller noget som helst. Og jeg har heller ikke automatiske varme justeringer på min radiator, kameraovervågning og alt sådan noget. Så jeg lægger måske snittet et lidt andet sted, end hvad jeg kan se i min omgangskreds.

[02:21] Dylan: Og tror du det her med, at folk har været kommunal længe, og de har haft de her arbejdsgange, de er vant til.. Vi så også mange forskellige opfattelser af det her cyber security. Hvor svært er det at få overbevist folk om, at de skal gøre det her ting? Det virker som om, at det er svært at komme ind til mange af medarbejderne?

[02:51] Medarbejder i databeskyttelsesteamet: Det er jo ikke deres kerneopgave. Deres kerneopgave er omsorg for borgerne i kommunen. Og det er det lige meget om du er tilknyttet park og vej, eller om du er tilknyttet hjemmeplejen eller skoleområdet. Det hele handler om, hvordan gør vi livet bedre for borgeren. Og det er svært at se, hvorfor de ikke må sende mails til store distributionslister. Hvad har det at gøre med servicen til borgeren? Det er nogle af de udfordringer vi har. Hvorfor skal de gøre de ting, vi siger, at det ligger alt for langt fra deres kerneopgave. Hvor vi prøver at holde fokus på, at I ikke kan udføre jeres kerneopgave, hvis I ikke husker databeskyttelse. Og det er jo i alt, hvad de laver. Det er jo de iPads, hjemmeplejen har med rundt. Det er de røntgen billeder, tandplejen tager af skolebørnene. Det er i det hele. Men det er jo også, når

borgeren melder ind, at lyset er gået på deres villa-vej. Og nu faldt deres mor og brækkede hoften og er nu indlagt. Så får vi på den måde en masse personhenførbare oplysninger, som jo også kan være følsomme eller fortrolige. Folk er utrolig glade for at skrive deres CPR-nummer, når de henvender sig. Og det har vi jo ikke brug for som udgangspunkt. I hvert fald så tager vi det hellere over telefonen, kan man sige. Så det der med at få det tydeliggjort, hvorfor det er vigtigt at huske og agere databeskyttelsesmæssigt korrekt for at kunne udføre sin kerneopgave.

[04:37] Så målet...

[04:39] Martin: Der er ikke noget specifikt for at udbrede den forståelse?

[04:46] Martin: Vores hypotese er også lidt, at den forståelse skal bare blive en normal del af hverdagen.

[04:56] Martin: At det ikke er noget, man tænker over, men ligesom at man skal ud og hente kaffe og arbejde.

[05:04] Martin: Det ligger så langt tilbage i baghovedet, at det bare er noget, man gør.

[05:09] Medarbejder i databeskyttelsesteamet: Det er jo et spørgsmål om vaner. Og jeg tror, det bliver nemmere og nemmere, fordi der kommer mere og mere fokus på det. Både i folks privatliv og på arbejdspladsen. Og det er jo lige meget, hvor man privat bor, men også hvor man arbejder henne. Og der ser vi jo, at folk hører... Altså, nu ved de godt, hvad en phishing-mail er. Jo, der er stadig folk, der klikker på den, men de ved godt, hvad det er. Som vi snakker om med sms'erne. De ved, hvad det er, og de ved, hvad man skal og ikke skal gøre. Det er mere, når vi kommer lidt dybere i det. Nu er de nået over begynderniveauet. Nu skal vi lige have dem på mellemniveau. Og det er det, vi springer i gang med at tage. Og det er svært at lave noget for alle. Vi har jo de her0 medarbejdere, hvoraf0 er administrative. Dem kan du stort set fange på en computer. Det er med e-læring, det er med mails osv. Skal du have noget ud på et plejehjem eller et plejecenter, så er det måske mere noget fysisk materiale. Og det skal være tilpasset til præcis deres hverdag, for ellers så læser de det ikke. De arbejder jo meget med kliniske instrukser, som skal leve op til en sundhedsmæssig standard. Og det er deres hverdag, det er de her instrukser og procedurer, som de arbejder ud fra. Når vi så kommer med noget og siger, at her er også en procedure for sikre adgangskoder, så i deres hoved er ordet procedure forbundet med noget andet. Så det er sådan en hel ændring af forståelsen af arbejdet. Så vi har meget fokus på at prøve at se, hvordan kan vi ramme de forståelser, Så vi har meget fokus på at prøve at se, hvordan kan vi ramme de forskellige medarbejdere, der hvor de er, men også i respekt for deres arbejdsopgave.

[07:07] Martin: Ja, det har vi også tænkt over. Det her med de forskellige forståelser af, lad os sige, cybersecurity awareness, at de forskellige forståelser også kan skabe, ligesom du siger, en barriere for at udbrede det.

[07:26] Medarbejder i databeskyttelsesteamet: Man kan sige, den helt grundlæggende ord, som I også skrev i mailen, jamen fokus er på cybersecurity awareness. Den formulering går bare ikke i Nordjylland. Jeg er selv fra Sjælland, så jeg må godt sige det. Den havde fungeret meget bedre derovre. Og når vi mødes på tværs af kommunerne og regionerne, man kan høre, hvem der arbejder på Sjælland, og hvem der arbejder i det jyske. Og det er der ikke noget galt i. Der er ikke noget rigtigt og forkert. Men der er en kæmpe forskel i, hvordan medarbejdere opfatter det. For hvis der kommer en sælger fra København og siger, jeg har det her fantastiske awareness-program, og det ene og det andet, og der er noget med augmented reality, og vi har nogle quiz-shows, og det er sat op til... Nå, det har jeg glemt det var, men jeg var nemlig til den vej til sidste uge, hvor der var en

sælger fra København, og han brugte en masse engelske termer for ting, som vi ville bruge danske termer for. Og det er en begrænsning, og det gør, at han ikke sælger til os. For når jeg skal ud og snakke med Bodil og Hans Christian og så videre, så skal jeg ikke komme og sige alt muligt på engelsk. Så skal det være, at det her betyder sådan og sådan for direkte jeres opgaver. Så hele den sproglige forståelse, og at vi har en meget forskellig virkelighed, det er enormt vigtigt, når vi gerne vil ud til folk.

[09:00] Heine: I forhold til at gøre det mindre perifert og mindre fluffy, og få dem til at forstå det mere, og gøre det mere konkret og lavpraktisk, hvad er måske nogle af de metoder, som du vælger at sætte i spil, for at prøve at overvinde dem, og få dem til at forstå de her ting, de skal gøre, og ikke få det til at virke som en hæmsko, men mere som en hej.. Nu nævnte du dig selv, at I skal gøre det her for at kunne udføre jeres arbejde, frem for at sige, at I skal gøre det her, fordi det siger jeg, at I skal gøre. Men ligesom for at vinde dem over?

[09:30] Medarbejder i databeskyttelsesteamet: Vi kan rigtig godt lide fysisk fremmøde. Det her med at møde op og tage en snak, være i dialog med dem. Hvis jeg kunne lave alt mit arbejde dialogbaseret, så gjorde jeg det. Lige nu hedder tilgangen, at når de kommer og spørger, må vi gerne købe et system, eller må vi købe den her dims, der kan overvåge et eller andet, så er mit svar altid nej. Men det ved dem, der oftest kommer og spørger mig også, de ved, at jeg siger nej, og så tager vi en snak om, hvad er det så faktisk, der kan lade sig gøre. Og det er egentlig for at sige, at nogen gange er det mig, der siger nej, og så er det min kollega Emma, som vi jo så mødte der. Så det er hende, der tager en dialog med dem om, hvad kan så lade sig gøre. Og så kan det være, at Emma og jeg har mødtes ved siden af, og har fundet en løsning til dem, og så er det hende, der præsenterer dem. Men det gør, at jeg bliver hende den sure, der siger nej, og Emma bliver hende den flinke, der hjælper dem. Og det lyder dumt. Men det gør bare, at det er nemmere for dem, fordi der er flere, der så går til Emma, i stedet for slet ikke at komme til os. Så på den måde har vi også forsøgt at sætte nogle roller, og det er altid nemmere at gøre hende fra Sjælland til den sure. De synes også stadig, jeg taler sjovt og sådan nogle ting. Og jeg har ikke boet på Sjælland i mange år. Men sådan er det bare. Og der spiller vi også på rollerne. Altså vi bruger det til vores fordel, at de ser mig som den sure, der siger nej. Og det gør også, når der er nogle medarbejdere eller en leder, der gerne vil have, at der bliver sagt nej, så kommer de til mig. Så vi bruger det som et aktivt værktøj. Men ellers så er det noget med at holde en masse dialog. Altså at komme ud og snakke med dem på afdelingsmøder eller sådan noget. Og så siger man, hvad er det, I oplever i jeres hverdag? Hvad er det i oplever i jeres hverdag? Hvornår har I sidst sendt noget forkert? Også intern sendt forkert. Det er også en sikkerhedshændelse. Den skal ikke anmeldes til datatilsynet, men det er en sikkerhedshændelse. Så vi skal have den håndteret. Og så gik det op for dem, at de havde tre, der hed Signe, tror jeg. Så dagligt sendte de forkert. Så skal vi måske lige have kigget på nogle mailadresser eller på nogle grupper, eller hvad er det, vi gør ved det? Og så tager vi udgangspunkt i deres hverdag. Så jeg opfordrer altid folk til at komme og sige, hvad er det, I har af problemer? Hvad er det, I oplever? Så udgangspunktet skal altid være deres hverdag.

[11:52] Heine: I forhold til deres hverdag og jeres viden, så er det jo ikke sikkert, at deres viden ligesom inkorporerer alle problemerne, der ligesom er. Så der kunne være en eller anden form for underlag af problemer, som du måske ikke siger, at I er med at kende til. Hvordan finder I så de problemer?

[12:10] Medarbejder i databeskyttelsesteamet: Altså, hvad man ikke ved, har man ikke ondt af. Og så kan man jo sådan sige lidt grovt. Forstå ved en måde, at vi griber de situationer, der kommer, når de kommer. Og så må vi håndtere dem. Det kan være, at det er et sikkerhedsbrud, der leder til, at

vi gør noget, at IT service desk er i gang med at hjælpe nogen, og så det hopper på deres skærm, og så kan se, at de har noget liggende på deres skrivebord. Det skal de ikke. Det kunne være, at vi lige skulle sørge for at hjælpe nogen med at finde ud af, hvad man så skal gøre i stedet. Vi er også gået i gang med et projekt om at få ryddet op på vores fælles drev, og der har folk jo gennem ting i, i hvert fald siden kommunens omlægning, så der har man gemt rigtig mange ting, og det har man bare gjort, for det plejede man at gøre. Så nu har folk fået øjnene op for, okay, det er ikke her, jeg skal gemme tingene, så skal jeg finde ud af, hvor skal de så ligge på mit eget OneDrive, eller er det noget, der skal ligge i Teams, eller skal de i fagsystemer osv. Og på den måde får vi også fundet nogle af de situationer, hvor folk bare har får vane og gemme forkert i steder. Så der sker stille og roligt ting, hvor man så finder ud af, at her var der lige noget, vi skal have samlet op på, og så kommer der nogen og siger, når man skal booke en borger til at komme ind i borgerservice, så skal vi faktisk have deres CPR-nummer skrevet i mødeindkaldelsen, for ellers kan det system med mødeindkaldelsen ikke tale sammen med standardsystemet nede i borgerservice, så når de kommer, kan standersystemet ikke fortælle dem, hvor de skal gå hen. Nå, okay, er der så en måde, vi kan løse det på? Så fik vi løst det og fundet ud af, at der var faktisk mulighed for at gøre noget backend, så det ikke kunne optræde osv. Så på den måde finder vi ud af tingene, når vi snakker med folk, og ellers så er det meget, at de kommer til os og siger, vi har det her problem, eller vi vil til at købe det her system, hvilke udfordringer er der i det? Og så siger vi, det kan I faktisk ikke grundet sådan sådan sådan, så siger de, det gør vi da i dag. Og så er det så, vi begynder at snakke om, okay, hvad kan vi så gøre i dag, eller hvorfor er det, I så ikke kan gøre det? Så på den måde er det faktisk ofte medarbejdere, der kommer med problemerne til os, og så er det på den måde, vi finder det. Andre gange så hører man noget hist og her, eller også så ved man bare, at på skolerne har de nogle udfordringer med et eller andet, og derfor har de begyndt at gøre noget andet, og det gjorde de så måske for 10 år siden, som en midlertidig løsning, men man har faktisk ikke fundet en permanent løsning endnu, så kunne det være, at vi skulle til at finde den permanente løsning.

[14:42] Dylan: Noget, vi har hørt meget om på tværs af vores interviews med medarbejderne, det var det her sikker mail, og det virker til, at der var også udfordringer med det, men ellers så virkede det til, at de alle sammen havde det, altså godt var klar over, hvordan man skulle bruge sikker mail, og vi fik ikke spurgt nok ind til, hvornår blev det implementeret, fordi det må have været en stor forandring på tværs af alle kommunale medarbejdere, de havde vel adgang til. . .

[15:16] Medarbejder i databeskyttelsesteamet: Det er jo alle offentlige, da man indførte e-boks eller digital post, der sagde man jo, at så skal der til at sende sikkert, og så har man helt lavpraktisk sat en knap ind, der hedder send sikkert, i stedet for en, der bare hedder send, og så er det den, man har lært medarbejderne at bruge, de er også blevet rigtig gode til at undersøge, om der er tunnel mail, ved I, hvad det er?

[15:45] Dylan: Du kan godt lige køre den igennem for os.

[15:50] Medarbejder i databeskyttelsesteamet: Tunnel mail er en måde med kryptering, så når jeg sender det, bliver det krypteret, og så er det krypteret, når det er i transit, og så bliver det pakket ud, når det rammer modtageren, hvis modtageren også er omfattet af tunnel mail, og så er det en sikker modtager, f.eks. offentlige myndigheder har alle sammen tunnel mail, så der er noget sikkerhed på den måde, men en g-mail, en hotmail, en live-mail, en aau-mail er ikke omfattet, så når vi skal sende på den måde, hvis vi skulle sende noget sikkert til jer, så ville vi sende til jeres private e-boks i stedet, eller til en virksomheds e-boks, og der var så meget fokus fra digitaliseringsstyrelsen og myndighedernes side, at det har man simpelthen bare kørt helt fast igennem, at det er noget af det første, du lærer, når du bliver elev, og når du bliver ansat, det er, hvad er som sagsbehandler, er det, du skal være opmærksom på, det er også en del af socialrådgiveruddannelsen, og alle

de her uddannelser, der leder ind til, at man bliver ansat i det offentlige, de har fokus på det forvaltningsretlige i det, og der falder så noget, som send sikkert også ind under, selvom man vil sige, at det er i stedet af noget databeskyttelsesretligt. Så der er en masse overlap på den måde, og det er jo bare gået hen og blevet hverdag. Vi har stadig sikkerhedshændelser, hvor man er kommet til at sende almindelige e-mails i stedet for at sende sikkert, og det kræver selvfølgelig lige noget opfølgning og noget kontakt til modtagerne, og de skal jo bekræfte, at alt ser ud, som det er osv. I nogle tilfælde skal vi orientere borgeren, hvis oplysningerne er sendt usikkert, men i de fleste tilfælde er det noget myndigheds, der er sendt, så det er alligevel at komme ud via tunnelmail. Så der er en masse arbejdsgangs, som medarbejderne får ind i løbet af deres uddannelse, eller i hvert fald i løbet af de første ganske få år, de er på arbejdsmarkedet.

[17:43] Dylan: Lige på falderebet, så tror du så, at det er jo en beslutning, der er kommet længere oppefra end jer Er det noget af det samme, at blive applikerbart til IT-sikkerhed? Føler du, at det burde komme ind på samme niveau? Tror du, det er nødvendigt, at det kommer opppfra en styrelse, politisk lagt ned over kommunen, hvor det rigtigt bliver kørt igennem?

[18:12] Medarbejder i databeskyttelsesteamet: Altså i min ideelle verden, så når man går i folkeskole, så bliver man undervist ikke kun i dansk matematik osv., men også i samfundsforståelse i bred forstand. Vi snakker både budgetter og sådan noget, men også i digital dannelse. Altså i forhold til hvad vil det egentlig sige og arbejde digitalt? Og det gør vi jo hele tiden, altså igen det her med smartphones osv. Min datter på knap fem synes det er fantastisk at sende Snapchat til sine bedsteforældre, fordi så kan hun lige vise, hvad hun laver. Og hun er ikke fem endnu, altså det er jo helt grotesk. Så allerede få det ind i folkeskolen med, hvordan er det egentlig, man gebærder sig, når man er online Ikke kun i forhold til opførslen, men også sikkerhedsmæssigt. Hvad er det for nogle vinkler, der er på det? Og så er det noget, der fastholdes op gennem uddannelsesniveau, og når man så når universitetsniveau, så vil jeg sætte baret lidt højere, måske også en smule teknisk, simpelthen for at få en forståelse for, hvilken betydning har det, når man bruger forskellige devices, men også hvad kan de devices bruges til af andre

[19:27] Dylan: Ja, der er vi helt enige. Det virker jo så basalt for os med en IT-baggrund, og det er jo det, der er lidt chokerende, når man kommer ud og snakker med, altså ikke at de er mindre vidende, men på det område, det er bare en sjov forskel. Selv da, vi snakker også med forældre, der er også meget generationsmæssigt i det. Så der er nok et længerevarende skift, der er nødvendigt.

[19:54] Medarbejder i databeskyttelsesteamet: Vi ser det hos de unge. Hvorfor skal der være adgangskode på min telefon? Altså jeg kan jo bare smække min tommelfinger på, eller mit ansigt på osv. Og ja, det kan du, men ikke på dit arbejdsudstyr, fordi den der lille device, du bruger til at sætte i din computer, den noterer så dine oplysninger. Og hvor kommer den device så fra? Er den amerikansk produceret? Er den kinesisk produceret? Hvem er det? Er softwaren lokal på deviceen? Eller er det noget, der ligger i skyen et sted? Hvis sky er det? Og hvor mange skyer, ja det. Så alle de der ekstra lag på det, ja det er skide smart at kunne smide fingeren på eller ansigtet på. Men som myndighed har vi også en forpligtelse overfor vores medarbejdere, sådan helt ansættelsesretligt, at vi må ikke overvåge dem på den her måde. Og hvis man går ind og siger, at for at komme ind i vores bygning, så er det ikke længere et adgangskort, så er det biometri, der tæller. Så kan vi godt notere, at den tommelfinger, der kommer på nu, den er godkendt til at komme ind de her steder, men I må ikke notere, hvem tommelfingeren tilhører. Hvis vi har et navn på tommelfingeren, så kan du jo overvåge mig og følge mig rundt i bygningen og min færden. Men hvis det er for at sikre, at præcis jeg har adgang til et eller andet lille arkiv eller et eller andet sted, og det er kun mig, der må komme derind, så vil alle jo vide, at det er mig, der har adgang, selvom man ikke har noteret navnet på tommelfingeren. Men giver det mening?

[21:33] Heine: Ja.

[21:35] Martin: Ja. Der kommer også lidt et ekstra lag på, når det er en myndighed, der skal stå for det her sikkerhed. Det er også meget spændende. Også det her med, at når data skal skifte hænder, at der også kommer et ekstra lag i sikkerhed. Hvordan man er sikker på, at en tredjepart også håndterer den her datasikkerhed og et netværk af forskellige organisationer, der skal have noget data, der skal være sikkert. Det er ret spændende.

[22:07] Medarbejder i databeskyttelsesteamet: I skal huske, at vi har jo en myndighedsforpligtelse. Men hvis vi fx lægger sundhedsoplysninger ind i vores fagsystem, så kommer Folketinget at have fundet på en eller anden bekendtgørelse, der siger, at det kan være skide smart, hvis vi kan sammenkøre sundhedsoplysninger fra alle kommunerne. Og så kan vi have noget statistik på, hvad det så er for en slags indsats, vi skal lave over. Så laver de en bekendtgørelse, der siger, at alle kommunerne skal smide deres data ind i den her klump. Og der er jo nogen, der skal forvalte den her klump. Hvem skal det være? Men de er jo bare en mellemstation, for så skal dataen videre til nogen andre, der så skal rent faktisk håndtere den. Så vi har ufatteligt mange politisk bestemte arbejdsgange, som ikke er GDPR-compliant og som ikke kan blive det i sådan lovmæssigt. Det er sort på hvidt forstand.

[22:59]Medarbejder i databeskyttelsesteamet: Hvor man siger, at det er vigtigt, at vi kan gøre de her ting. Så derfor laver vi en politisk bekendtgørelse, der siger, at nu skal I gøre det. Og det giver også god mening. Jeg er kæmpe fan af samarbejdet, det er slet ikke det. Men vi skal bare kunne styre strømmen af data, og det kan vi ikke, når vi så bliver pålagt og overført til nogen, som så ikke ser sig selv som dataansvarlig, men som en dataformidler, hvilket ikke er et term, der findes i lovgivningen, men som egentlig så er data behandler. Men er de så selvstændig dataansvarlige, eller er det overhovedet en databehandler af konstruktion? Er det en videregivelsesituation i stedet? Og jeg er ikke jurist, og jeg bliver forvirret af det, og det er mit arbejde. Så jeg kan godt forstå, at Bodil og Hans Christian nu i forvaltningen, de synes, det er noget fis, at de skal være opmærksomme på alle de her ting. Så det er et spørgsmål om simpelthen at have rigtig meget dialog med dem, og så gribe dem, når det går galt. Altså når de får lavet et sikkerhedsbrud eller sådan noget, så får snakket med dem om, hvad er det, så der er sket. Altså vi vil helst ikke have, at medarbejdere går grædende hjem.

[24:13] Dylan: Ja, jeg tror ikke, vi har mere. Du snakkede sådan om, at der kunne være, når vi sagde Cyber Security Awareness, så var der mange forskellige forståelser. Hvis nu du skulle prøve at give din forståelse af, hvad du tænker, at Cyber Security Awareness betyder. Bare sådan kort, hvis du kan det.

[24:37] Medarbejder i databeskyttelsesteamet: Jeg gør ikke kort.

[24:40] Martin: Det må også godt være langt, så. For mig, så er det opmærksomheden omkring databeskyttelse i bred forstand. Det er alle aspekter af det. På alle platforme og på alle måder. Og det er alt for uhåndgribeligt, når jeg ser det på den måde. Så vi gør meget i at kassetænke. Forstået på den måde, hvad er det for nogle problematikker, vi har lige nu, og hvad kan vi gøre ved dem specifikt. Og så må vi tage det lidt af gangen. Vi er, Ulla har 15 timer. Emma har i princippet en 50Og så de andre 50Og jeg sidderSå vi snakker under to fuldtidsstillinger til at håndtere en mellemstor kommunes databeskyttelsesarbejde. Der skal prioriteres benhårdt. For mig handler det om at se på databeskyttelsen fra medarbejdernes synspunkt. Og hvordan kan jeg hjælpe dem til at gøre deres arbejde. Databeskyttelsesmæssigt mest compliant. Tror jeg nok. Sådan en kort beskrivelse.

[26:08] Dylan: Ja, det er noget af en opgave.

[26:12] Medarbejder i databeskyttelsesteamet: Men det er også spændende, fordi du ved aldrig. Jeg har lige afvist et telefonopkald fra en. Jeg venter angående et sikkerhedsbrud. Jeg kan se, at der kommer et andet ind også her, mens vi sidder og snakker. Så jeg ved også, at jeg har hele tiden noget at lave. Og en gang imellem, så er det, at de har sendt forkert internt. Og andre gange, så er det de større sager, som vi også ser i medierne. Så jeg bliver også betalt for at være på arbejde hele tiden. Og har fået stillet udstyr til rådighed. Så jeg er netop hen over påsken og ferie generelt. Så skal jeg lige tjekke. Ligger der noget i postkassen, er der kommet noget ind, der skal håndteres? 72 timer fra vi opdager det, til det skal være anmeldt. Det har kæmpe betydning henover fem helligdage, vil jeg bare lige sige. Altså bare en weekend kan være enorm belastende for et undersøgende arbejde i forhold til, hvad der er sket. Så jeg har ikke to dage der er ens. Emma ynder og siger, at jeg arbejder kun ad hoc.

[27:09] Dylan: Ja, brandslukning.

[27:11] Medarbejder i databeskyttelsesteamet: Ja, stort set. Du kan godt have en plan for, hvad du skal lave, når du møder ind. Men det er ikke sikkert, at det overhovedet har noget at gøre med det, du ender med at lave. Og det synes jeg er rigtig, rigtig spændende. Også fordi jeg får lov at snakke med rigtig mange, forskellige steder i organisationen. Og om mange forskellige ting. Hvem vidste, at der fandtes drikkeglas, der kan registrere, hvor meget mængde der er i. Og hvilken type væske er det, der er i. Hvor mange gange er glasset blevet løftet og så videre. Det er jo genialt i forhold til dem, der har svært ved at få væske. Men det er lige noget med, hvor meget vi så egentlig registrerer om borgerne. Og hvad står der i glasene og så videre. Så det er jo også de her utrolig gode hjælpemidler. Men vi skal bare lige have dem lige en smule lovliggjort.

[27:57] Martin: Det er godt nok også vildt alt det, man kan registrere og have data på. Så det er jo alting snart. Hvor meget vand man drikker. Det er godt nok vildt.

[28:08] Medarbejder i databeskyttelsesteamet: Men det er sgu et godt værktøj. Men vi fandt også en løsning. Der var slet ikke nogen problemer. Men hvad skal der egentlig stå i den? Jamen det kunne være rart, hvis borgeren havde sit navnstunde og sit CPR-nummer og så videre. Men det var faktisk ikke nødvendigt. Vi kunne godt kalde glaset for A1. Og så noterede man i fagsystemet, hvem der havde glas A1 den pågældende uge. Så for så ligger oplysningen i vores fagsystem. Så har vi også opfyldt journaliseringspligten og journalføringen. Så jeg tænker meget ind i det også.

[28:45] Dylan: Ja, for der er jo et mismatch, med at sige, at folk har jo... I skal indsamle den her data, for det er borgerens ret. Men I må heller ikke indsamle dataen for meget. Så det er meget balancegang.

[29:01] Medarbejder i databeskyttelsesteamet: Ja, og selvom det har været for borgerens eget bedste. Vi har indsamlet de her oplysninger om, hvad de har fået at drikke. Så må vi ikke bruge oplysningerne til andet, end præcis den borgers journal. Altså det kunne da være super fedt, at alle de her glas afgav en masse data. Vi kunne lave noget statistik på, hvad er det så for en form for væske, de måske helst drikker. Hvornår på dagen drikker de det helst og så videre. Varmt, koldt, alle de her ting. Super fedt, hvis man kunne gøre det. Men det er bare ikke det formål, vi har indsamlet data til. Og hvis vi gør det, så er det profilering og overvågning. Og det går ikke. Så en almindelig lille henvendelse om et glas kan kaste rigtig mange ting af sig.

[29:36] Dylan: Ja, spændende.

[29:39] Medarbejder i databeskyttelsesteamet: Men det er skide spændende, hvis I spørger mig.

Men nu er jeg også lidt nørdet i lige på det her område.

Interview slutter

A.6 Interview - Medarbejder 2 i databeskyttelse (Rekonstruktion)

Arbejder i databeskyttelsesteam'et - de er mere strategisk anlagt i forhold til data end eksempelvis IT-afdelingen, der i højere grad tager sig af hændelser når de opstår.

Forstår cybersecurity awareness som dét, at være opmærksom på cybersecurity, lade det være en fast del af hverdagen i organisationen og holde sig opdateret hele tiden

Der er mange forskellige forståelser i organisationen, hvilket skaber udfordringer. Der er flere medarbejdere, hvor det ikke er en del af deres primære arbejdsopgaver

Medarbejder i databeskyttelsesteamet 2 mener, at det skal indlejres i kulturen i organisationen og hos de enkelte individer ved at sætte fokus på cybersecurity awareness. Det er ikke blot en opgave for IT-afdelingen, men det er dog dem, der skal være bedre til at få alle med på det.

Hun mener, at oplysning omkring cybersecurity kan være en vej frem. Dette er dog ikke kun oplysning omkring de tekniske aspekter, men også på værdien af cybersecurity awareness, da de fleste i organisationen ikke mærker en direkte værdi i deres arbejdsdag.

Foretrækker at have en dialog fremfor e-læring eller pixiebøger

Gulerod frem for pisken, guleroden kan forekomme i form af humor eller ros når bruddene bliver anmeldt

Hun har ikke noget imod at bære "nej hatten", for hendes kollega Louise har mere en "ja hat" på, hvilket skaber en god dynamik i forhold til at tilføje nye tiltag og opretholde de igangværende tiltag i forbindelse med CSA. Hvis der er noget som ikke kan tilføjes, eller et forslag bliver afslået, så finder de i fællesskab en løsning, som kan overholde diverse restriktioner for at sikre cybersikkerheden.

Hun mener at CS og CSA skal være et undervisningsemne på lige fod med personlig økonomi og skat

I og med, at der generelt bliver større og større fokus på cybersecurity, også i privat øjemed, tror Medarbejder i databeskyttelsesteamet 2 også, at der automatisk vil komme større fokus på at være bevidste omkring det i organisationer. Især, da næsten ingen jobs er uden berøring med nogen former for IT.

A.7 Interview - Afdelingsleder, sekretariatet (rekonstruktion)

De første tre ord: Vigtigt, relevant, besværligt

Valget faldt på disse ord, da hun mener vigtigheden og relevansen er vigtigere nu end nogensinde før. Hun mener det er et besværligt emne, da det er fluffy og det er svært at få medarbejdere til at forholde sig til, da det ikke er et decideret facit og arbejdet er kontinuerligt.

De sidste tre ord: Taknemmelig, Samarbejde, besværligt

Efter interviewet nævnte hun taknemmelighed og samarbejde. Hun er taknemmelig for at samarbejdet er så omfattende, så de føler de på bedst mulig vis kan bearbejde de potentielle problemer som kan opstå og møder lille modstand, når der er tiltag der skal implementeres. Der er en stor forståelse af vigtigheden af CSA, selvom det er besværligt at implementere, så samarbejder de for at få den bedst mulige løsning ud af det.

For at imødekomme modstand mod forandring er hun for guleroden og imod pisken. Guleroden bliver indført ved blandt andet at have humor, være åben og hjælpes med at finde en fælles løsning på et givent problem. Før i tiden gav de slikposer ud, for at hjælpe medarbejderne med at huske på forskellige tiltag, såsom cybersecurity og CSA.

Sproget er alfa omega, hvor hun mener at sproget og kulturen er noget nært det samme i hendes tilfælde ift den daglige arbejdsdag. Sproget og kulturen går hånd i hånd. Sproget skal tilpasse det personel, som skal modtage informationen.

Hun nævner at der ikke kan sættes et facit under CS og CSA, men at det er en kontinuerlig proces. Derudover, så er de meget ansvarsbevidste og ved at nogle medarbejdere lægger ansvaret over på dem, men er ved at arbejde på at få medarbejderne selv til at anse, hvordan de selv har en indflydelse på det, og at det i en hvis omfang også er en del af deres ansvar. Ved at de er åbne og imødekommende har de derfor en kultur, som gør at medarbejderne ikke er bange for at hive fat i dem, når det kommer til problemer som skal løses.

Hun fremhæver at fysisk fremmøde og i-person dialoger er en af de bedste redskaber de har, når det kommer til at forklare om og implementere CS og CSA.

A.8 Interviewguide

1. Fortæl lidt om dig selv og hvad du laver
2. Intro + forklar formålet
   Forklar, at det ikke er dem specifikt vi ønsker at undersøge, men CSA i en større kontekst
3. Skriv 3 ord ned, når du hører ordet cybersecurity (Post-it)
4. Hvad er dit kendskab til cybersecurity?
5. Hvis vi siger cybersecurity awareness, hvad tænker du så?

   Ved du hvad målene for de angreb er? Er det noget du tænker over til hverdag? Bevidst/u-bevidst?
6. Hvad vil du mene det betyder at være “aware” i forhold til cybersecurity?
7. Tror du, der er forskellige opfattelser af CSA her i organisationen? Hvis ja, hvilke? og hvorfor?
8. Hvilken betydning tror du, det har?
9. Hvor vigtigt synes du CS og CSA er?
10. Fylder det for meget/for lidt i din hverdag? Hvorfor/hvorfor ikke?
11. Hvor meget kender du til, hvordan sensitive data bliver sendt, opbevaret og håndteret i din arbejdsgang?
12. I hvilke dele af din arbejdsdag kommer CS og CSA til syne?
13. Skriv 3 ting ned som du tager med fra det her interview eller som du tænker mere over Hvorfor lige de tre ting?

A.9 Ekstraction sheet

Transkribering og udvalg af citater

Kodenummer	Interviewperson	Timestamp	Citat	Analysefelt	Note
1.1	Skolelærer	01:45	Cybersecurity for mig er i hvert fald noget med at forebygge og være sikker på, at man er på forkant med de ting, der kan ske i organisationen, som vi er i.	Forståelsesrammer	Hans udvalgte ord inden interviewet startede
1.2	Skolelærer	01:55	Men det handler også om, at der er nogen, der tager ansvar for at få fulgt op på det og sørge for, at sikkerheden er i orden.	Domæneanalyse	
1.3	Skolelærer	02:26	Tofaktor genkendelse er også noget, vi får besked på, om det er en god idé at have i forhold til vores maskiner, med GDPR og alle de informationer, vi har på vores maskiner, og vi også har på vores drev.	Awareness Modenhed	
1.4	Skolelærer	03:04	Når jeg hører det, så tænker jeg jo, at det er det her med at være bevidst om, at det er noget, der er vigtigt. Det tror jeg faktisk ikke, at det er mange, der er. Dem, som måske har en lille smule IT-snille, de ved nok godt, hvad det handler om. I min organisation, der vil jeg tro, at 80% af vores stab, vil nok ikke helt vide, hvad det handler om. Det er bare slag på tasken.	Forståelsesrammer	
1.5	Skolelærer	04:15	Jeg tror, jeg er mere bevidst om, hvilke søgmaskiner jeg bruger, når jeg browserer på nettet. Jeg er bevidst om, hvilke apps jeg giver tilladelse til, på min telefon for eksempel. Jeg er bevidst om, hvad jeg siger, hvornår, i forhold til, om der er nogen ting, der optager det, jeg siger. I forhold til algoritmer og sådan nogle ting.	Awareness Modenhed	
1.6	Skolelærer	06:21	Jeg tror i høj grad, det er det. At man ikke lige helt ved, hvad det er. Er det noget teknisk, eller er det ikke noget teknisk? Har jeg egentlig forståelse, eller har jeg viden omkring det? Nej, det har jeg måske nok ikke. Så bliver det nedprioriteret på en eller anden måde. I forhold til de andre ting, der foregår i løbet af sådan en hverdag.	Forståelsesrammer	
1.7	Skolelærer	07:01	Det fylder jo ikke meget. Det er nok mere i min underbevidsthed, tror jeg. Jeg tror ikke, jeg synes, det skal fylde mere for mig. Men jeg tror måske, at jeg synes, det skal fylde mere på bredt plan. At der er flere, der er klar over det, og flere, der er med på, hvordan vi gør for at forhindre de ting.	Forståelsesrammer / Inkongurens	
1.8	Skolelærer	07:36	Det tror jeg, der er mange her, der gør. Jeg tror, der er mange, der tænker, at vores IT-mand, han styrer det der. Faktisk. Det er nok de 80 procent, der er, som jeg nævnte før.	Forståelsesammer / Inkongurens / Domæne	

1.9	Skolelærer	08:12	Det tror jeg, det er kun bare det her med at få det afmystificeret på en eller anden måde. Sådan at alle, mere eller mindre, ved, hvad det handler om. Det tror jeg, jeg ville gøre meget ved, at det var noget, man også kom til at snakke om. Og noget, der var mere fokus på hos alle medarbejdere. Og dem, som har en idé om, hvad det handler om.	Awareness Modenhed	Kan bruges i både awareness, og forståelsesrammer
1.10'	Skolelærer	08:42	Det er et svært spørgsmål. Det er et rigtig svært spørgsmål. Også fordi, at der er mange, som i det her fag synes tiden er knap. Og det der med at få de rigtige ting ind. Også specielt, når det er noget, der måske skal foregå ud over den hele arbejdstid. Så er det faktisk rigtig, rigtig svært at finde ud af, hvordan og hvor ledes kan man det. Men det kunne da sagtens være... Altså det der med bare lige at sidde med et program, den ved jeg ikke. Men det med at få belyst det på en eller anden måde. At der er nogen, der kommer og fortæller om det. Sætter fokus på det på en anden måde måske. Det tror jeg godt, man kunne nå langt med.	Awareness Modenhed	
1.11	Skolelærer	09:39	Hvis der kommer sådan nogle informationer, som der jo gør engang. Så er det jo også ofte noget, der kommer ind på AULA, vores platform. Hvor det ligger i en oversigt eller i en besked. Der er jo nogen, når de læser, om der står noget med cyber eller der står noget med IT. Så er der nogen, der allerede er videre til næste besked. Så det der med, at det sådan er et eller andet, der bliver stablet på benene. Hvor det er en eller anden person, der kommer og ligesom gør opmærksom på det. Og fortæller om det. Det tror jeg i hvert fald er en bedre vej end det andet.	Awareness Modenhed	
1.12	Skolelærer	10:35	For mit vedkommende ja. Jeg er samfundsfagslærer blandt andet. Og jeg er også engelsklærer. Og det er noget, jeg tager fat i af og til. Men det er ikke noget, der sådan fastlagt i boende ligger i nogen former. For årsplaner eller noget som helst. Så det er noget, jeg tænker, man skal selv have lysten til. Ligesom at tage det op med klassen. Men jeg synes jo, det er enormt vigtigt. Fordi som du selv siger, internettet er bare et farligt sted. Men det er ikke noget, alle gør langt fra. Jeg tror heller ikke, det er ret mange her på stedet, der tager det op. I deres undervisning aktivt. Selvom det er enormt vigtigt.	Domæneanalyse	Det var hans svar ift at blive spurgt om undervisning i internet brug i folkeskolerne
1.13	Skolelærer	11:53	Jeg tror i hvert fald lige med lærer, sikkert med rigtig mange andre mennesker også. Det skal give mening. Der skal være en idé med, at vi sidder over to timer på at høre om cyber security eller hvad nu.	Awareness Modenhed	

1.14	Skolelærer	12:56	Jeg tror bare, at det er, at man er bevidst om, at uanset hvad du laver på nettet nærmest, så er der nogen, der tracker dig, der er nogen, der ved, hvad du laver, og der er nogen, der kæmper om at få din information, altså at få din opmærksomhed. Og den går til højeste udbyder, kan man sige. Det er i hvert fald nogle af de ting, som jeg sætter fokus på, når vi snakker om det. Og så hele tiden det her med, at det er bare nemt at komme i klemme muren til, hvad man laver online. Alt det her med anonymiteten og sådan noget. Så det er noget, jeg har rigtig stort fokus på. Også i forhold til nu nævnte de også TikTok og apps og sådan nogle ting. Altså hvordan navigerer man dem bedst, det er helt klart sådan noget, som jeg sætter fokus på.	Forståelsesrammer	
1.15	Skolelærer	17:23	Nej, det jeg ved, det er noget, jeg selv har holdt frem til eller har undersøgt. Og ja, der er ikke noget fra skolens side eller noget som helst.	Awareness Modenhed	
1.16	Skolelærer	18:29	Ja, det tror jeg godt, men igen, det er fandme et svært segment at overbevise om ting, og det er bare virkelig meget det her med, at det skal give mening. Der skal være en mening med det, og jeg tænker netop det, vi talte om før, at hvis man kan vinkle det på en sådan måde, at det jo egentlig også er for børnene skyld for at gøre dem klogere på det, at fange dem tidligt, hvis man kan sige det, så de bliver bevidste om, hvordan man undgår, eller man forsøger for at blive her tænkt, så tror jeg faktisk, det er en rigtig god vinkel. Men det er selvfølgelig stadigvæk, tror jeg selvsagt, at dem, der er mere IT eller teknik interesseret, de vil nok tage det mere til sig, end Hans Christian på 67, som går på pension om 3 år, hvis I kan følge mig i den. Men jeg tror, det er helt klart vejen at gå, det skal give mening, og det skal give mening på en eller anden måde nu og her, selvom det selvfølgelig også giver mening at passe på sine informationer i organisationen.	HHAFAPS	
1.17	Skolelærer	20:38	Det er der helt sikkert nogen, der vil. Der er jo nogle, hvor det er de mindste ændringer i det, man plejer at gøre. Der kan være træls. Hvis det er noget, man i forvejen har lidt svært ved, så jo, det ville det da sikkert, men det er jo også noget, der forholdsvis er uskyldigt, så jeg tror egentlig, at man godt kunne implementere det, og så ville der være nogen, der brokker sig, og så ville det gå over. Det kunne jeg godt forestille mig. Jeg tror ikke, at det er noget, der ville vedvarende være bekymringer eller irritationer omkring. Også hvis man snakker om, hvorfor er det, vi gør det.	Awareness Modenhed	
1.18	Skolelærer	21:43	Det tror jeg godt, det kunne med tiden, og måske også allerede nu. Vi lever bare i en tid, hvor flere og flere ting digitaliseres, og lige pludselig, så er der jo ikke ret mange ting, vi gør fysisk længere. Så helt sikkert, så ville det da i min optik tage en plads sammen med de ting der. Og det er jo let for mig at sidde og sige, fordi jeg gør jo lidt af det i forvejen, kan man sige. Men ja, hvis I spørger mig, så ja. Uden tvivl.	HHAFAPS	Hans svar på om CS og CSA skulle være en del af pensum

1.19	Skolelærer	23:30	Jeg tror lige det der med vidensdeling, det kom faktisk lige fordi, at vi jo er nogen, som egentlig sidder med lidt viden, men egentlig ikke rigtig sådan, som vi også sagde, vi får ikke rigtig snakket om det. Der kunne jeg måske godt, eller det kunne mine kollegaer måske også godt, tage til den, og så lige få snakket lidt omkring det, og egentlig finde ud af, hvor folk står i det. Og så det sidste, det var jo i forhold til det, vi snakkede om, at hvis man skal i gang med at implementere eller gøre folk klogere på det, så er det i hvert fald bare vigtigt, at det ikke er en besked på AULA, men at det ligesom er et eller andet, der bliver gjort, og noget, der har et islet, der giver mening i forhold til, hvorfor sidder vi og hører eller bruger to timer på det her. Ja, for at forsøge at forebygge eller forsøge at blive klogere på at være helt sikkert.	Forståelsesrammer	Hans uddybelse af de 3 udvalgte ord efter interviewet
2.1	Afdelingsleder i handicapområdet	02:01	Nu har jeg været en del af det her med at lave en hjemmeside indenfor mit område og jeg er mest bekendt med gdpr i forhold til det her med billeder, fordi vi har Facebook, vi har hjemmesider, instagram, vi har alt muligt som profilerer os og fortæller om, hvordan er det at være handicappet i Hjørring Kommune og, hvad laver vi rent faktisk	Forståelsesrammer	De tre ting hun skrev ned til at starte med
2.2	Afdelingsleder i handicapområdet	02:01	Og så er det også det her med, at så må vi ikke gemme alle navnene i den samme sag. Det er vel en del af journaliseringsdelen, det kan godt være, jeg blander det en lille smule sammen. Når vi laver lister med CPR-numre som vi skal bruge til noget aftjekning så må de ikke ligge sammen og altså, alt det der, som kan komme til at fylde i hverdagen, hvor det ville være nemt, hvis man bare lige kunne... men det kan man så ikke. Altså det er det, der fylder for os	Awareness Modenhed	
2.3	Afdelingsleder i handicapområdet	02:01	Jeg har været i alle forvaltninger, hvor vi bruger forskellige systemer i de forskellige steder i forvaltningerne. Så jeg bliver også optaget af, at da j eg engang for 15 år siden sad ovre i jobcentret, der havde man et system, hvor man rent faktisk havde adgang til andre afdelinger, børne- og familieafdelingen eksempelvis.	Awareness Modenhed	
2.4	Afdelingsleder i handicapområdet	02:01	Så jeg synes, det er vigtigt, men det bliver også lidt tungt. Så for mig er det både det ene og det andet.	Forståelsesrammer	
2.5	Afdelingsleder i handicapområdet	07:13	Altså, at man er særlig obs på det som udviklingen det byder på. Jeg tænker på, det handler om at udviklingen, den rykker sig hele tiden, så vi skal være sikre på, at når vi introducerer nye systemer eller nye teknikker, eller der kommer et nyt medie, noget vi ikke kan forudsige konsekvenserne af, der skal man være særlig opmærksom på, at.. jeg går ud fra, det er det, jeg ved det ikke. Det er gætværk	Forståelsesrammer	
2.6	Afdelingsleder i handicapområdet	07:48	Det er i virkeligheden det, det handler om. At det her, det går hurtigt. Det er superfedt. Der er masser af teknikker, der kommer til at hjælpe os både i pleje og administrativt. Men hvad gør det ved os både i relationerne, hvis vi begynder at bruge teknikker i forskellige robotter, hvad gør det så med relationsarbejdet og så er der hele den administrative del, hvad gør det ved mig, hvad efterlader det af spor på mig, når jeg forsvinder ud af den her kommune, ud af det her liv eller hvad vi forsvinder ud af.	Forståelsesrammer	
2.7	Afdelingsleder i handicapområdet	08:29	I hverdagen tænker jeg ikke ret meget over det. Jo, på helt lavpraktisk niveau, tænker jeg over det. ugh, jeg er begyndt at afvise cookies, fordi jeg tænker sådan, det skal man nok. Man gør det sådan lidt hovedløst, indtil jeg fandt ud af, jeg får det samme ind på mine medier. Men jeg gør det lidt hovedløst. Desværre.	Forståelsesrammer / Modenhed	
2.8	Afdelingsleder i handicapområdet	11:37	Men jeg synes, det er mega spændende fordi at ting kan blive besværlige, men jeg er også bange for, at det der awareness kommer til at begrænse os i udviklingen	Forståelsesrammer	

2.9	Afdelingsleder i handicapområdet	13:21	Nej, men jeg synes, det giver noget pangel. Det bliver sådan lidt tungt, nogen gange. Men det er fordi, jeg forstår godt, hvorfor vi skal bruge det. Når jeg så skal videreformidle til min personalegruppe, hovedsageligt håndværkere over 50. Når jeg skal formidle de her ting så bliver det lidt tungt.	Awareness Modenhed	
2.10'	Afdelingsleder i handicapområdet	13:57	Nej, jeg giver dem de små tips. Jeg gør det nemt, i skal huske det, det og det, så jeg tager dem i små punkter ud fra, hvad jeg piller ud, hvad de skal være opmærksomme på.	Awareness Modenhed	Hvordan hun selv gør sine medarbejdere aware
2.11	Afdelingsleder i handicapområdet	14:49	Men det kan godt være, vi mangler sådan nogle awareness programmer som man lige kunne køre igennem. På vores onboardingplan for eksempel. Husk lige, vær opmærksom på. Ligesom man gør med tavshedspligten.	Awareness Modenhed	
2.12	Afdelingsleder i handicapområdet	17:33	Jeg opfatter mig som forholdsvist kvik, så når jeg får sådan en så sender jeg den til IT, fordi det regner jeg med at mine kolleger også gør, så hvis der er et mønster, så samler de det og sender ud, hvis vi skal være opmærksomme på det. Det er dem der har den der sammenhængskraft for alle os, der er ansat i kommunen.	Forståelsesrammer / Domæneanalyse	
2.13	Afdelingsleder i handicapområdet	19:27	Altså mine 103 medarbejdere som er dem der er førtidspensionister har ikke en kommunal pc eller noget. Mit personale de har selvfølgelig. De fører også fakturering og følgesedler og sådan noget, og samarbejde på kryds og tværs, så det fylder da også i deres hverdag. Men det er faktisk ikke noget vi drøfter. Vi kunne godt bruge mere tid på det.	Awareness Modenhed	
2.14	Afdelingsleder i handicapområdet	20:58	Altså sådan en historie har jeg fortalt fordi den er skideskæg, men det er ikke sådan at vi på ledermøder for eksempel lige drøfter er vi udfordret på noget sikkerhedsmæssigt. Det gør vi ikke. Så er det noget, der kommer oppe fra. I skal være opmærksomme på et eller andet, eller fra IT. Så er det noget vi skal forholde os til og så gør vi så det. Men det er ikke sådan at vi har jævnlige møder om vi overholder det ene og det andet.	Domæneanalyse	
2.15	Afdelingsleder i handicapområdet	22.32	Det tænker jeg, at de tænker, at det først er vigtigt når jeg begynder at skrive ud, at det giver kage på deres regning. Vi havde sådan nogle kurser, hvor jeg tog den der genvej med mig. Der drillede man hinanden på kryds og tværs med det.	Awareness Modenhed	
2.16	Afdelingsleder i handicapområdet	23:17	Jeg tænker ikke, at hvis jeg spurgte i mit ledelsesteam, så kender de ikke den der (hentyder til windows+L), og jeg har heller ikke sagt, at vi skal huske det.	Awareness Modenhed	
2.17	Afdelingsleder i handicapområdet	29:06'	Ligeså snart der CPR-numre og adresser, så hvis det skal sendes ud af kommunen, så sender jeg det herop og så sender de det ud af kommunen som sikker post. Jeg vil have at det er en anden der gør det med sikker post	Forståelsesrammer	
3.1	Demenskonsulent	01:35	Det første, det er, at jeg tænker, at være sikker at mail, og dele personlige oplysninger. Og så tænker jeg også det der, når jeg får noget ind i min inbox, hvad jeg siger jeg til? Hvad hedder det? Skal jeg bare skrive det, som jeg har samtidigt tænkt på? Hvad accepterer jeg i min inbox?	Forståelsesrammer	Svaret på hendes 3 udvalgte ord
3.2	Demenskonsulent	02:28	Det er meget af de tre ting, jeg lige tænker, ja. Den sidste ved jeg, at man klikker på, og når man går ind og søger på et eller andet på sin arbejdscomputer, eller hvad er det for nogle links, man klikker på, og hvad skal man acceptere, og hvad skal man ikke acceptere? Det er det, jeg tænker, at man skal være opmærksom på, for awareness må være at være opmærksom på noget.	Forståelsesrammer	

3.3	Demenskonsulent	03:04	Det er noget, jeg får at vide af mine børn, jeg skal. Altså, nogen siger bare, bare tryk OK til det hele, ikke også, og andre de siger, pas lige på. Hvad er det, du trykker på, og klikker på, og hvis det er noget, du er usikker på og sådan noget, så ja. Jeg får jo nogle gange nogle mails om, at på min arbejdsmail, du har ikke hentet den og den pakke, eller du har vundet et eller andet, hvor jeg tænker, det skal jeg i hvert fald ikke lige klikke på, fordi det er helt sikkert, for jeg har ikke bestilt nogen pakke over mit arbejdsmail, så det er i hvert fald ikke noget, jeg lige...	Awareness Modenhed	
3.4	Demenskonsulent	03:43	Det er bare en sund fornuft, jeg tænker, at over min arbejdsmail, der har jeg ikke bestilt noget, og hvis jeg bestiller noget over min privatmail, så ved jeg jo, hvad det er, jeg har bestilt, og hvornår det kommer. Så hvis ikke jeg har bestilt noget inden for de sidste par dage, så vil jeg ikke gå ud og hente noget.	Awareness Modenhed	
3.5	Demenskonsulent	04:39	Ja, og det man selv opsøger selvfølgelig også jo. Men meget af det, der kommer ind, sådan... Hvem er det, der har sendt den? Ja, det er det. Ja, og vi har jo det der for eksempel... Hvis nu, hvis jeg sender en mail ud af kommunen, eller for eksempel til æl Det er jo rigtigt. Så får jeg jo sådan en, du vil sende mail ud af systemet, ud af vores organisation, ikke? Og så kan jeg sådan, okay, det er det rigtige sted, jeg sender den hen. Så det er vel også det, der er været opmærksom på, hvor man sætter tingene hen, ja.	Awareness Modenhed	
3.6	Demenskonsulent	05:36	Vi får jo lige den der lille reminder, du vil sende mail ud af organisationen. Og det var faktisk i forbindelse med det første, med det sikre mail der. Jeg gik faktisk med en tanke om, at man aldrig måtte sende fx personnummer, men det må man så godt have internt i kommunen, fordi det er sikker mail.	Awareness Modenhed	
3.7	Demenskonsulent	06:30	Det ved jeg faktisk ikke, fordi jeg har ikke nogle umiddelbare kollegaer sådan lige.	Domæne	
3.8	Demenskonsulent	08:45	Ikke sådan lige, nej. Det er som, hvad man ellers finder ud af gennem tiden. Ja, der skal man ikke sende hen, og der kan man godt sende hen, og ja, så må man jo så spørge et eller andet sted.	Awareness Modenhed	Hendes svar på om de får træning
3.9	Demenskonsulent	09:41	Ja, det tror jeg faktisk, det bliver sådan lidt... At så hører man måske nogle historier om, at det er gået galt for nogen, fordi de har fået klikket på et eller andet forkert link eller sådan noget, ikke? Og så tænker man, at det skal man nok lige lade være med. Ja. Men det er jo ikke sådan noget, altså. Det er bare det der cyber-awareness, det var jeg ikke engang klar over at det var et begreb, tænkte jeg. Okay, hold da	Forståelsesrammer	

3.10'	Demenskonsulent	11:36	Altså, jeg synes jo, det kunne være dejligt, hvis vi kunne kommunikere alt. Til for eksempel lægerne og ældre psykiatrien. Hvis alt det foregik over journalsystemet. Fordi så vidste vi jo, ligesom det var samlet et sted. Ja. Og så tænker jeg, der er nogen her inde i det her hus, der har styr på, hvordan det fungerer. Så jeg kan være helt trygt på, at her kan du skrive lidt. Naturligvis biviste om, at der kan komme noget på, og at der kan komme nogen, der skal have adgang til det. Så man skal selvfølgelig også være opmærksom på, hvad man skriver. Men at du ligesom kan dele ting. Og adgang til de samme informationer for eksempel. I stedet for, fordi ældre psykiatrien for eksempel ikke har adgang til vores journalsystem. Så det bliver jo sådan lidt dobbelt arbejdet. Der er mange ting, vi skal gøre flere gange.	Domæne	
3.11	Demenskonsulent	15:49	Men vi bliver ikke oplært i det. Det var jo helt tilfældeligt det der. Jeg tror faktisk, det var fordi, der var et eller andet, jeg var inde her ved IT. Og så, hov, du har altså gemt din kode, det må du jo ikke. Nå, men så skal jeg jo sidde og huske det hver eneste gang, og når man så skifter sig i det måde, hvad man var nu lige, det var altså noget ikke. Så er det meget lettere, at den lige er gemt. Og det må du altså ikke. Nå, okay. Det var jeg jo ikke klar over. Hvis ikke jeg havde været herinde, så kunne der jo endelig være nogen, der havde snubbet Og du skal jo bare... Fordi jeg får jo de der SMS'er engang imellem om, at du har ikke hentet, eller du har ikke... Den pris, du har vundet i et eller andet i Lottisystem, den har du ikke afhentet. Den SMS kan jeg godt få, ikke? Og hvis de har adgang til min telefon, kan de jo også meget nemt få adgang til, fordi der er min kalender faktisk også på. Så har de jo nemt adgang til min kalender om dermed mange andre ting, ikke? Hvis jeg for eksempel sagde, nå, det var da mærkeligt, jeg har ikke det. Jeg må heller lige skynde dig at klikke, hvis det er, at du ikke vil have den sendt tilbage, eller hvad nu de skriver, ikke?	Awareness Modenhed	
3.12	Demenskonsulent	18:01	Ja, jeg mener, det hver 6. måned. Så kommer der sådan en advarsel et par dage før, at nu den bliver udløbet. Det skal jeg jo hver eneste gang. Hver gang. Når jeg åbner min computer, jeg har en fastnets-computer, og så har jeg en tablet, og så har jeg en telefon. Ja, min telefon den har bare en kode Men for eksempel tablet, hvis jeg skal gå ind på vores journalsystem, så skal jeg jo hver gang logge ud, hvis jeg skal logge ind på en nyt center, og der er jo så tretten i kommunen. Og der skal jo være, jeg tror, det er 10 bogstaver, og det er to eller tre tal, ikke også? Og det må ikke være én, du har brugt inden for de sidste 3 år eller sådan et eller andet, hvor man sådan tænker, at det er der, hvor jeg bliver nødt til at have en lille seddel i min telefon. Og så kan jeg ikke huske det for gang i gang, hvor jeg nu er kommet til i min...	Awareness Modenhed	Hendes svar da hun blev spurgt ind til passwords

3.13	Demenskonsulent	26:10'	Men jeg hører jo også til den generation, der ikke er opvokset, altså jeres generation, og dem, der kommer efter. De er jo opvokset, men det er bare en naturlig del, er det ikke? Ja. Mit barnebarn her var jo ikke mere end tre før, da han vidste, hvordan han låste sine forældres telefoner op og sådan noget, de er jo næsten født med telefonen i hånden i dag, eller bl.a. eller andet, ikke? Så der er måske der, man skal sætte mere ind, fordi vi, ja, det ved jeg ikke.	HHAFAPS	Her hentyder hun til vigtigheden af undervisning i CS hos mindreårige
3.14	Demenskonsulent	32:28'	Ja, hvad hedder så noget? Jeg skriver lige sikkert mail igen, men det er det, der er med, men... På samarbejdspartere også, det var lige. Og det kunne faktisk også godt være... Det der med, at journalsystemet taler sammen. Det må I gerne bringe videre, hvis det er.	Modenhed	Hendes sidste 3 noter efter samtalen
4.1	Bibliotekar	01:44	Jeg har skrevet GDPR, Keylogging og hacking, og det er sådan noget som er. Det er ligesom tre begreber som er taget ud af min virkelighed, min arbejdsvirkelighed kan man sige.	Forståelsesrammer	Hans tre ord
4.2	Bibliotekar	02:09	Ja, hvis vi tager dem en ad gangen, GDPR det er bare sådan noget jeg kan mærke, jeg har været i biblioteksbranchen i nogle år og det er bare sådan noget, hvor der bare er blevet skruet på en knap, hvor man lige pludselig er kommet i tanker om, hov det kan måske være vi sidder, altså vi er bare et bibliotek, men vi har måske adgang til nogle systemer, noget data som er følsom for nogen, det er sådan den ene del af det, det er noget jeg kan mærke er blevet eskaleret. Og så keylogging, det er fordi der har været i vores branche nogle mega uheldige sager lige nøjagtigt med det, det er sådan noget vi har brugt mange timer over at tænke på hvordan man håndterer sådan noget, på en meget lavpraktisk måde som også kan fungere i hverdagen. Og så hacking det er fordi jeg sidder med hjemmesider, sociale medier og sådan noget, og det er bare, det er sådan noget jeg tænker på en gang imellem. Og hvor der også, jeg sidder med i sådan nogle nationale netværk, hvor man kan se kolleger i andre kommuner, hvor de bare sådan mister det hele, så ja.	Forståelsesrammer	Uddybet svar på de tre ord
4.3	Bibliotekar	03:24	Medium til OK vil jeg sige, det er sådan lidt svært at sætte en eller anden, hvad kan man sige, 0 til 100 på ikke altså, jeg bilder mig ind at jeg synes jeg har rimelig styr på sikkerhed et eller andet sted, men så er det også en cybersecurity, når I siger det kunne man måske også, det er så der jeg tænker, hvordan definerer vi det, altså fordi det er bare så mega bred en paraply at det er jo alt muligt. Det er jo sådan noget som det her, men det er også alt muligt andet, så det jo i hvert fald i min optik. Så jeg tror og håber at jeg har sådan en rimelig god forståelse af det, men som man så også kan se og som der har været ufatteligt mange eksempler på efterhånden synes jeg, det er at når man ligesom tænker der er styr på det her pis, det er der bare ikke. Det er jo en kontinuerlig proces, så det er jo ikke sådan et mål kan man sige.	Forståelsesrammer	
4.4	Bibliotekar	04:30	Jamen jeg tror, jeg mener faktisk lidt det som jeg, det man kan sige med processen, at man ikke er færdig, man kan ligesom godt tænke at vi er dækket af, at vi sådan har brandsikret eller prøvet sådan at fremtidssikre os lidt mod et eller andet, men der er jo bare, der sidder bare nogle kloge mennesker et eller andet sted med nogle rimelig trælse hensigter også, som nok skal komme videre end det. Så derfor skal vi også bevæge os hele tiden, altså og så kan man sige, hvad er det? Og det ved vi måske ikke fordi den ikke er bygget endnu. Giver det mening?	Forståelsesrammer	

4.5	Bibliotekar	05:05	Det tror jeg er meget uforsigtigt og påstå at man tænker nu er der styr på det. Der er altid nogen som nok skal komme med et eller andet counter, øh, modoffensiv som tænker, hvordan får vi prikket hul i det, eller nårh de har ikke tænkte på det ovre i hjørnet eller noget i den stil. Men ja, altså jeg tror jeg kan mærke sådan i mit arbejde at det i hvertfald er noget over tid, hvor man bliver mere og mere, ja aware, er jo nok ordet. Altså sådan med hvor meget skal man passe på og hvad er det nu, er det nu en god ide at vi får lavet det her på den måde, eller burde jeg sende den her ting eller sådan noget i den stil. Lige nu er vi for eksempel igang med en migration fra sådan nogle servere og fællesdrev til at flytte det hele over i OneDrive og i den oprydningsproces har vi sådan nogle scanningsværktøjer som IT har til at køre, der sådan lige scanner alt vores mails og dokumenter igennem for lige at få se, har vi noget der ligger som vi måske ikke skal have til at ligge. Altså bare sådan helt basic, der er vi helt nede på bunden synes jeg og der vælter jo frem med ting og sager fordi man, fordi der er hverdag og man kan godt gå og tænke, det skal vi også lade være med at gøre og vi skal gøre sådan her. Men det skal også være færdig klokken et i dag, så jeg skynder mig lige og lave et eller andet.	Forståelsesrammer	
4.6	Bibliotekar	07:03	Mmm, ja, altså hvis man nu tager udgangspunkt i de her ting for eksempel (hans tre punkter), nu tager vi keylogging, altså der har vi haft, der er rigtig mange mennesker som bruger biblioteket som en print central, hvor man går ned og printer fordi det ikke kan betale sig at have en printer derhjemme, men vi har lukket af for alle vores USB porte, fordi det er ligesom den primære adgang til keylogging. Øhm og så bliver man lige pludselig meget bevidst om når folk kommer med deres USB pinde og siger “Kan jeg få det her ud”, nej det kan du ikke. Der bliver det ligesom inkorporeret i en hverdag der fungerer på en eller anden måde, men også tilstedekommer noget brok og diskussioner, noget med publikumservice, altså det der med, det plejer vi jo at kunne og det kan vi lige pludselig ikke længere, ergo serviceforringelse sådan noget i den stil. Men også sådan noget, det er rimelig paradoxalt, hvis man tager GDPR tingen, vi har i en del år haft et, vi har et fagsystem, et biblioteksfagsystem, når vi slår dig op for eksempel (peger på Heine), så ser vi hvor du bor henne og sådan noget, og vi ser dit CPR nummer og så siger du at du gerne vil bestille Nietzsches samlede værker, et eller andet kommer du og siger, og den har vi ikke selv så jeg sender den lige til en eller anden, og så før i tiden, for uhyggeligt kort tid siden, der ville vi have sendt dit CPR nummer i en mail der ikke er krypteret, ja, men i fagsystemet, altså vi snakker i nyere tid ik, men i fagsystemet har du et eller andet nummer som man ikke kan bruge til en skid overhovedet, som kun duer (virker) inde i vores fagsystem og det er så det jeg skulle sende til nogen, kan du ikke lige reservere til låner osv osv. Men det der personhenførbare data altså at der ligesom er kommet en bevidsthed, som ligesom er blevet inkorporeret i dagligdagen, hvor det så fungerer på en måde, hvor folk egentlig også kan se at det kunne godt være vi lige…	Domæne	
4.7	Bibliotekar	09:07	Ja, man kan sige beskyttelsen udadtil, den er todelt hos os, fordi vi har jo ligesom, vi har en IT infrastruktur hos os, men den er ude i en armslængdeprincip fordi at vores infrastruktur, altså i huset, den bliver lavet hernede et eller andet sted, vi bor jo et andet sted, så det er lidt distanceret på en eller anden måde, det er ikke sådan noget vi, det er meget kommunalt ikke, det er noget IT de tager sig af, det fikser de nok, det er sådan den ene del af det. Men så har vi så vores, hvad hedder det, vores fagsystem, vores biblioteksystem, vores hjemmesidedrift og det er ligesom, det kører et andet sted fra, så det er sådan, jeg tror måske nok det måske er en lidt usund tankemæssigt at det er distanceret og ikke er noget vi selv har styr på, men samtidigt med så ved jeg at dem som sidder i den anden ende og tager sig af det, de har markant mere styr på det, altså vi har ikke ressourcer til at have IT personale der kan styre sådan noget, men det gør måske også lidt at sådan tankesætsmæssigt, så er det ikke så present i hverdagen, der er styr på det regner vi med.	Domæne / Forståelsesrammer	

4.8	Bibliotekar	10:45	Nej jeg tror faktisk lige netop ikke, det kan godt være det er paradoksalt i forhold til mange andre steder, men jeg synes ikke vi har været ude i noget med at det er blevet egentligt mere besværligt, men det er bare sådan noget med at man skal gå fra sådan noget "vi plejer" til nårh nu skal du lige gøre det på den her måde, fordi om jeg skal finde dit CPR nummer inde i vores bibliotekregister eller om jeg skal finde dit lånernummer som det så hedder, sådan et randomt genereret nummer det er samme forskel arbejdsmæssigt, men det er det bare ikke for din datasikkerhed kan man sige. Der har vi været sådan rimelig heldige. Så er der måske noget med for eksempel det der med at vi har lukket af for alle USB porte, en anelse mere besværligt, men når man så snakker med folk om det, og vi fortæller dem det er fordi sådan og sådan, at der er nogen som har mistet jeg ved ikke hvor mange penge og sådan noget fordi de har, fordi de er blevet keylogget, så er folk jo med på at, altså dialogen, og så kommer der måske et ok resultat ud af det i 90% af tilfældene ik, og så i de sidste der ikke kan få printet et eller andet ud, de finder nok på et eller andet andet	Modenhed / HHAFAPS	
4.9	Bibliotekar	12:00	Vi har snakket lidt om det på vores kontor, for jeg tror at jeg synes det er meget, nu er det også selvfølgelig her, hvor jeres fagterm er et eller andet sted, men som jeg ser det så er det, det der med at man sådan har det ligesom at det ligger underbevidst på en eller anden måde. At man sådan er, at der sådan en, hvad kan man sige, en underliggende tanke om, et eller andet man skal passe på. Det kan både være internt, men det kan også være noget eksternt, men måske også en, det ved jeg ikke, verden er jo et rodet sted pt, at ting er mere sårbare måske, end man sådan lige regner med, og man skal jo ikke bladre i ret mange aviser før man ser nu er det her nede, den her er blevet hacket og sådan noget i den stil. At noget man sådan har tænkt der er meget robust før, det er måske der den ligger i awareness tingen, at der er sådan en instabilitet, skrøbelighed indbygget sådan samfundsmæssigt også lige pludseligt, at man ikke skal regne med noget og SAS går ned eller et eller andet i den stil. Altså der er ikke noget som er sikkert, sådan længere på en eller anden måde. Så derfor får man også lyst til måske at sikre sig så godt som man kan ikke, og ja, giver det mening	Forståelsesrammer	
4.10'	Bibliotekar	14:09	Nej det tror jeg netop ikke jeg kan faktisk, jeg synes det er sådan helt randomt. Hvor man har læst om her fornyligt en eller anden hackergruppe som lægger udenrigsministeriet ned bare for at sige det kan vi. Altså sådan på den måde så bliver det noget, så er det noget magtdemonstration, men selvfølgelig er der også, der er ikke kun magtdemonstration i det, der er også noget med at hvis man kommer ind i nogle systemer og man så har adgang til alt muligt, så kan man sige, vi på biblioteket har nogle personfølsomme oplysninger og vi har noget lånerhistorik faktisk en lille bitte grad. Det har vi så ikke så meget længere, fordi det har vi også fået skåret væk, så jeg kan ikke se hvad du har lånt for tre måneder siden for eksempel noget i den stil.	Awareness Modenhed	
4.11	Bibliotekar	15:05	Det er sådan en GDPR ting. Paradokset er så at man kan slå det selv, altså hvis du selv bruger vores app for eksempel, så kan du gå ind og sige, prøv lige at gem min historik, så hvis du tænker har jeg læst det her før, et eller andet i den stil, så kan du slå den til fremadrettet.	Modenhed	
4.12	Bibliotekar	15:59	Fuldstændig, for hvor går grænsen ik? Altså man kan sige at bomber er meget håndgribeligt, men hvis du nu bare læser de forkerte bøger på en eller anden måde, hvis du er voldsomt fascineret af en eller anden yderligtgående politiker eller sådan noget og du bare har styr på det hele, du har lånt alt, eller sådan noget i den stil, eller bare sådan noget Mein Kampf, som du har fast udlån på nonstop. Og det er jo også, man kan jo sige, biblioteket er også pakket ind i en ideologisk skal om der skal være fri og lige adgang for alle og der skal ikke være nogen som er mere eller mindre overvåget end andre. Vi leverer det og så er det ligesom den frie tanke der opererer derfra, så det er sådan lidt, hvor godt det passer sammen med sådan en, ja for eksempel en overvågning, efterforsknings kontekst ikke særlig godt kan man sige, men altså det er så ude i en etisk diskussion et eller andet sted	HHAFAPS	

4.13	Bibliotekar	17:33	Helt lavpraktisk, så har vi jo et biblioteksrum, altså vi har låste døre ind til vores kontorer og sådan noget, det skal man have og vi skal låse vores computere når vi går fra dem, det skal man, det siger Ulla som sidder lige herude. Men det giver også god mening fordi de står åbne med adgang direkte ind til kommunens IT infrastruktur, så hvis man får fat i en af vores computere, og ved hvad man laver, så har man altså adgang til en del. Men sådan noget som det at lige at trykke lås når man går, den er svær. Allerede der bliver det svært. Så kan man sige, det er spændet på awareness-delen, den viser det faktisk meget godt, at der er nogen, jeg er sådan lidt fascistoid omkring det og låser også andres computere, hvis jeg lige kommer forbi en, så siger jeg lige plup og så, men der er også andre som tænker, årh det går nok, jeg skal bare lige herover.	Awareness Modenhed / Forståelsesrammer	
4.14	Bibliotekar	18:28	Det ved jeg ikke, jeg ved det simpelthen ikke, fordi så skal man til at låse op igen, det er også lidt besværligt og sådan noget i den stil. Lidt besværligt. Men jeg tror faktisk det der med, det er spændet ik, er der forskel på det, ja der er virkelig forskel på det og jeg er også, jeg vil være meget uforsigtig hvis jeg sadge at der ikke bliver sendt nogen som helst emails med CPR numre nede fra os.	Awareness Modenhed	
4.15	Bibliotekar	19:17	Ja, altså det er jo så heldigvis, kan man sige, begrænset, jeg er faktisk ikke engang selv helt klar over, hvor meget data jeg har adgang til, fordi jeg har ikke undersøgt, lad os se hvor langt vi kan gå ud på drevet, jeg har ikke gået i gang med den øvelse, men jeg går ud fra og håber på at der er nogen nede i IT, som har sat nogle begrænsninger op på mig og på min bruger, på hvor galt det ligesom kan gå.	Domæneanalyse / Awareness Modenhed	
4.16	Bibliotekar	19:59	Ja, det kan man godt sige på den måde, men det er også en almindelig driftssituation, Martin er ansat på biblioteket, han skal have adgang til de her mapper og han skal have adgang til de her systemer, det synes jeg er en meget logisk måde at lave det på. Det er det samme når jeg sidder og laver hjemmesider og jeg skal give adgang til en af jer, så får du redaktøradgang og så skal jeg nok sørge for at du ikke kan pille inde i coren af et eller andet dopa system eller sådan noget i den stil, det skal jeg nok selv gøre.	Domæneanalyse	
4.17	Bibliotekar	20:51	Jamen jeg tror, hvis det giver mening for jer, altså awaredelen for mig er, det er sådan en bevidsthed om at man sådan, to ting, at man skal opføre sig ordentligt, passe på og at ting kan gå galt og så de to ting er der selvfølgelig en vækselvirkning, så hvis man ikke gør sit arbejde ordentligt, på en eller anden måde, det tror jeg awaredelen er for mig, man gør det jo ikke for hyggens skyld	Forståelsesrammer	
4.18	Bibliotekar	21:25	Ja, jeg tror konsekvenserne er svære og overskue, men at der kan være en konsekvens egentlig, på den måde, og at man på den måde egentlig, jeg tænker når, i min hverdag, når man arbejder med nogen systemer, hvor man så har, det er sådan respekt overfor dem som bruger biblioteket på en eller anden måde, at man ligesom opfører sig ordentligt, passer på deres ting ik. Det ville være det samme hvis jeg var en mekaniker og nogen kom og afleverede deres bil, så passer jeg også på den, altså på den måde ikke. At man sådan ligesom, jeg tror det er det, at man sådan er et ordentligt mennesker, hvis man skal op på en eller anden etisk platform, men ja, det kan man jo også sagtens være uden at være aware kan jeg godt se, men ja, jeg tror det er det, et eller andet sted, at der er en respekt for det man laver og det måske er sådan et middel på en eller anden måde, ikke et mål, aldrig et mål, men et middel til en del af den oplevelse for dem som jeg ligesom skal servicere og det arbejde jeg skal lave, at man er, ja opmærksom.	HHAFAPS	

4.19	Bibliotekar	23:00	Ja det vil det være, altså nede hos os, det er så igen det der med at vi er et led ude, fordi vi er nede på biblioteket og det her er kommunen, men ja det ville det være. Det er jo vores chefer og vi har så også haft Ulla, som I lige har snakket med heroppe også, nede hos os og lige have en gennemgang af hvad er det for nogle scenarier vi kan være ude i og hvordan kan vi meget meget let, helt lavpraktisk komme en god del af det til livs altså, men det der med at få informationer til at sive ud i en hverdag, det er bare, det du kan edermandme skriver mange mails om sådan noget. Et eksempel, jeg laver også grafik og kommunikationsarbejde på biblioteket også, jeg har egentligt mange hatte på, men på et tidspunkt havde jeg lavet sådan en plakat, sådan noget med at man skulle give kage hvis man glemte at låse sin computer og den tænkte vi at vi simpelthen ikke kunne sætte op, fordi så meget kage kan vi slet ikke håndtere. Men altså, det er sådan noget man kan se blive bedre, for når vi så har haft besøg af Ulla for eksempel og det bliver italesat, så har man det måske i en, det er måske ikke det man snakker over hver dag over frokosten, men at det ligesom er, at der er et frø som er sået og så kunne jeg godt, jeg er sådan lidt firkantet, så jeg kunne godt tænke mig at vi siger fra på onsdag låser alle kraftædeme deres computere og låser også andres når de går forbi den, men sådan fungerer virkeligheden bare ikke, det tager tid og gøde den her awareness åbenbart ikke.	Forståelsesrammer	
4.20'	Bibliotekar	24:41'	Fuldstændig, men noget som også gøder det er jo for eksempel sådan noget som nyheder, når man så ser at alt muligt bare bliver hacket fra en side af, eller at der har været brud på et eller andet, det ville jeg så også våge at påstå at er med til det implicit. At folk kommer i tanker om, som jeg også nævnte før at verden er bare mere usikker end man måske tror.	Forståelsesrammer	
4.21	Bibliotekar	25:18'	Det er top vigtigt synes jeg, ja, helt sikkert, men også fordi vi er sådan et, måske i forhold til andre organisationer, så biblioteket er bare gennemdigitaliseret, altså meget af det vi laver, alle transaktioner, vi har engang imellem, hvor vores biblioteksystem går ned, ikke hacket, men der er nedetid, og når der er det, så går organisationen mere eller mindre i stå, altså man kan godt finde nogle bøger frem manuelt, men du kan ikke låne dem ud, du kan ingenting. Det er bare så meget vores organisation og være digital og der kunne jeg forestille mig at det kunne gå knap så galt hvis man er i en børnehave eller et eller andet i den stil, så ja, det fylder.	Awareness Modenhed	
4.22	Bibliotekar	26:10'	Jamen det er det og samtidigt med at, det hænger også lidt sammen med perifært sammen med jeres opgave, så kan man også, den anden dag for eksempel, i lørdags der havde vi mistet forbindelsen til CPR registeret, som så betyder at vi ikke kan oprette en ny låner for eksempel, fordi vi ikke kan hente info og så er der sådan lidt, hvorfor. Før i tiden ville man bare være inde på en eller anden statusside, der vil være noget nedetid, der er nok nogle teknikkere som går og roder med et eller andet. Men nu der er det sådan, kan man også mærke at det er og det er også en del af awarenesstingen at, hmm, er der sket et eller andet som ikke skulle være sket, og skriver rundt til alle mulige kollegaer i andre kommuner, har I det samme problem, og de har også det samme problem, det er en national ting, der et sket et eller andet og så er der endelig en som finder et eller andet med, hvor der står nårh, forresten vi har noget opdaterings et eller andet.	Forståelsesrammer / Awareness Modenhed	
4.23	Bibliotekar	26:58'	Jamen, det tror jeg faktisk at det er noget jeg er begyndt mere med at før havde man bare tænkt, nåh ja, servicevindue eller et eller andet, men selv at sådan nogle kritiske ting, altså forbindelsen på CPR registeret er ret kritisk for os, og for ret mange, og hvis man har lagt det ned, så er der godt nok mange ting der ikke fungerer lige pludselig, og det er også sådan en baglæns awarenessdel et eller andet sted, at man, at det er ikke meget sådan noget ulven kommer, men mere at ulven den er her, altså tænker man sådan helt automatisk først, før man	Forståelsesrammer / Awareness Modenhed	

4.24	Bibliotekar	28:09'	Altså, hvordan det fungerer i vores fagsystem? Altså det bliver sendt krypteret i hvert fald og vi har det ikke som sådan, vi har sådan et datapoint vi har der ligger et eller andet sted, hvor vores fagsystem kan kigge ned i gennem en sikker forbindelse, det cirka så meget jeg ved om det. Jamen også sådan noget som sendt frem og tilbage, for så er det nemlig den der, vi arbejder i to. Vi har sådan et fagsystem vi arbejder i, men hvis vi skal sende bestillinger til andre biblioteker, så skal man ud af det og så over i et andet krypteret system, men det er så der man har muligheden for at for eksempel sende CPR nummer, det er ikke noget, der er potentielt nogen som kan få fat i det, men det er der, hvor man skal vælge de her lånernumre, men hvordan det bliver sendt og sådan noget, jeg går ud fra at der er styr på sikkerheden, men jeg ved det ikke sådan helt konkret.	Domæneanalyse	
4.25	Bibliotekar	29:28'	Ja, altså man kan sige, vi har jo ikke dataen som sådan, man kan ikke gå ned og stjæle en computer nede ved os og så har man alle vores låneoplysninger, det kan man ikke, så er det mere den daglige drift, altså håndteringen af det, og det synes jeg er top vigtigt. Så kan man sige at IT afdelingen, det er mere infrastrukturen på en eller anden måde, de har jo ikke håndteringen af dataen som sådan, men det er mere sådan at de har lavet et ordentligt system nede hos os håber jeg. Men jeg har tænker egentligt også på, nej men det er fordi jeg bliver ved med at tænke over det der overvågning og de der bomber, at der er jo også, nede hos os, det er jo så også en anden del, som der er en del der bruger, vi har åbne WIFIs for eksempel nede hos os, som er noget der har været snak om i nogle år, hvorfor har man et åbent WIFI og hvorfor har man det ikke så man skal logge på, så vi kan se hvad du laver. For der har vi nemlig haft nogle eksempler på at IT afdelingen lige pludselig står der, så der foregår også en eller anden form for overvågning, altså den datatrafikmæssigt, altså hvor de siger, hvem er det der sidder ved computer sådan og sådan, for vi kan se at der sker et eller andet.	Domæneanalyse / HHAFAPS	
4.26	Bibliotekar	30:50'	Jo, det har vi også noget med arbejdere i fagsystemer i hvert fald, så skal vi, eller vi kan kun, det kan kun fungere hvis vi kører på en VPN forbindelse og det er et meget fint benspend og specielt kan man sige, post-corona er der ret meget hjemmearbejde, jeg arbejder enormt meget hjemme, men der er det en god løsning til at man ikke sidder alle mulige steder nede på en eller anden random cafe	Awareness Modenhed	
4.27	Bibliotekar	32:21'	Altså helt lavpraktisk i min arbejdsdag, lige om lidt når jeg er færdig med at snakke med jer, så skal jeg jo ned og passe biblioteket altså ude i udlån, og der er det en del af det, for der står man jo med, inde i systemet, men ude i et offentligt rum. Det er sådan noget, det tænker jeg i hvert fald over, når man arbejder med det også, vi har en meget meget åbent bibliotek, vi har nede hos os, folk kan kigge med sådan inde over skulderen og sådan noget, ja også sådan noget med, hvad man sender til folk. For der bliver bare sendt utroligt meget mellem biblioteker, vi har sådan noget interubant samarbejde og hvad der bliver sendt der, det er især der hvor vi passer på synes jeg.	Awareness Modenhed	
4.28	Bibliotekar	33:55'	Der er to af dem, der er sådan en jeg har skrevet lokalfoanrking, men det er faktisk det der, det kan jeg godt se at, det der med ansvarsdelen, hvor ligger ansvaret henne, fordi det er super let bare at sige at IT tager sig af det, at det er deres problem, men måske er det også ens eget problem, eller det er det jo. Og den hænger lidt sammen, nu har jeg skrevet PC lås, jeg tror måske vi skal have en lille kampagnetur nede hos os, det kan godt være jeg skal have kageplakaten op alligevel. Nu er der så mange som låser deres computere at vi ikke kommer til at drunker fuldstændig i kage. Og så den der GDPR ting, jeg har skrevet GDPR igen fordi det er sådan en, den er bare altså det er der, hvor vi sådan kan behandle data ordentligt, på en eller anden måde, det er der, hvor vi virkelig har sådan, altså hvordan de bliver håndteret og hvordan de bliver sendt rundt	Forståelsesrammer	
5.1	Medarbejder i databeskyttelsesteamet	01:06	Det er, at folk i det kommunale ofte har været i det kommunale længe, eller i hvert fald i det offentlige.	Domæne	
5.2	Medarbejder i databeskyttelsesteamet	03:12	Og det er svært at se, hvorfor de ikke må sende mails til store distributionslister.	Awareness Modenhed	

5.3	Medarbejder i databeskyttelsesteamet	04:14	Folk er utrolig glade for at skrive deres CPR-nummer, når de henvender sig.	HHAFAPS	
5.4	Medarbejder i databeskyttelsesteamet	05:27	Altså, nu ved de godt, hvad en phishing-mail er. De ved, hvad det er, og de ved, hvad man skal og ikke skal gøre. Nu er de nået over begynderniveauet. Nu skal vi lige have dem på mellemniveau. Og det er det, vi springer i gang med at tage. Og det er svært at lave noget for alle.	Forståelsesrammer	
5.5	Medarbejder i databeskyttelsesteamet	06:11	Skal du have noget ud på et plejehjem eller et plejecenter, så er det måske mere noget fysisk materiale. Og det skal være tilpasset til præcis deres hverdag, for ellers så læser de det ikke. De arbejder jo meget med kliniske instrukser, som skal leve op til en sundhedsmæssig standard. Og det er deres hverdag, det er de her instrukser og procedurer, som de arbejder ud fra. Når vi så kommer med noget og siger, at her er også en procedure for sikre adgangskoder	Awareness Modenhed	
5.6	Medarbejder i databeskyttelsesteamet	07:35	jamen fokus er på cybersecurity awareness. Den formulering går bare ikke i Nordjylland. Og når vi mødes på tværs af kommunerne og regionerne, man kan høre, hvem der arbejder på Sjælland, og hvem der arbejder i det jyske. For hvis der kommer en sælger fra København og siger, jeg har det her fantastiske awareness-program, og det ene og det andet, og der er noget med augmented reality, og vi har nogle quiz-shows, og det er sat op til... Nå, det har jeg glemt det var, men jeg var nemlig til den vej til sidste uge, hvor der var en sælger fra København, og han brugte en masse engelske termer for ting, som vi ville bruge danske termer for. Og det er en begrænsning, og det gør, at han ikke sælger til os. For når jeg skal ud og snakke med Bodil og Hans Christian og så videre, så skal jeg ikke komme og sige alt muligt på engelsk. Så skal det være, at det her betyder sådan og sådan for direkte jeres opgaver. Så hele den sproglige forståelse, og at vi har en meget forskellig virkelighed, det er enormt vigtigt, når vi gerne vil ud til folk.	Forståelsesrammer / Awareness Modenhed	
5.7	Medarbejder i databeskyttelsesteamet	09:30	Vi kan rigtig godt lide fysisk fremmøde. Det her med at møde op og tage en snak, være i dialog med dem. Hvis jeg kunne lave alt mit arbejde dialogbaseret, så gjorde jeg det.	Awareness Modenhed	
5.8	Medarbejder i databeskyttelsesteamet	17:10	Vi har stadig sikkerhedshændelser, hvor man er kommet til at sende almindelige e-mails i stedet for at sende sikkert, og det kræver selvfølgelig lige noget opfølgning og noget kontakt til modtagerne, og de skal jo bekræfte, at alt ser ud, som det er osv.	Domæne	
5.9	Medarbejder i databeskyttelsesteamet	18:12	Altså i min ideelle verden, så når man går i folkeskole, så bliver man undervist ikke kun i dansk matematik osv., men også i samfundsforståelse i bred forstand. Vi snakker både budgetter og sådan noget, men også i digital dannelse. Altså i forhold til hvad vil det egentlig sige og arbejde digitalt?	HHAFAPS	
5.10'	Medarbejder i databeskyttelsesteamet	24:43:00	For mig, så er det opmærksomheden omkring databeskyttelse i bred forstand. Det er alle aspekter af det. På alle platforme og på alle måder ... For mig handler det om at se p		
5.11	Medarbejder i databeskyttelsesteamet	05:40	Og det er jo i alt, hvad de laver. Det er jo de iPads, hjemmeplejen har med rundt. Det er de røntgen billeder, tandplejen tager af skolebørnene. Det er i det hele. Men det er jo også, når borgeren melder ind, at lyset er gået på deres villa-vej. Og nu faldt deres mor og brækkede hoften og er nu indlagt. Så får vi på den måde en masse personhenførbare oplysninger, som jo også kan være følsomme eller fortrolige		
5.12	Medarbejder i databeskyttelsesteamet	04:26	Så det der med at få det tydeliggjort, hvorfor det er vigtigt at huske og agere databeskyttelsesmæssigt korrekt for at kunne udføre sin kerneopgave		
2.18	Afdelingsleder i handicapområdet	19:25	Afdelingsleder i handicapområdet: Det er mest der, hvor jeg opdager, at jeg ikke har tænkt mig om. Altså cookies, og så opdager jeg pludselig, at nu føler jeg mig lidt indskræn		

A.10 Ekstraction sheet - kodning

CSA Kultur	CSA Forståelse	Awareness Modenhed	HHAFAPS
1.2	1.1	1.5	1.10'
1.8	1.4	1.6	1.18
1.12	1.6	1.7	3.13
2.7	1.7	1.9	4.7
2.12	1.8	1.10'	4.12
2.14	1.14	1.11	4.18
3.1	1.19	1.13	4.25
3.3	2.1	1.15	5.3
3.8	2.2	1.17	5.9
4.2	2.4	2.1	
4.4	2.5	2.2	
4.6	2.6	2.3	
4.7	2.7	2.4	
4.15	2.8	2.7	
4.16	2.9	2.9	
4.19	2.11	2.10'	
4.24	2.12	2.11	
4.25	2.17	2.13	
4.27	3.1	2.15	
5.4	3.2	2.16	
	3.9	3.3	
	4.1	3.4	
	4.2	3.5	
	4.3	3.6	
	4.4	3.8	
	4.5	3.11	
	4.7	3.12	
	4.9	4.8	
	4.13	4.9	

	4.17	4.10'	
	4.19	4.13	
	4.20'	4.14	
	4.22	4.15	
	4.23	4.18	
	4.28	4.2	
	5.4	4.21	
	5.6	4.22	
	5.10'	4.23	
	5.11	4.26	
	5.12	4.27	
		5.2	
		5.4	
		5.5	
		5.6	
		5.7	