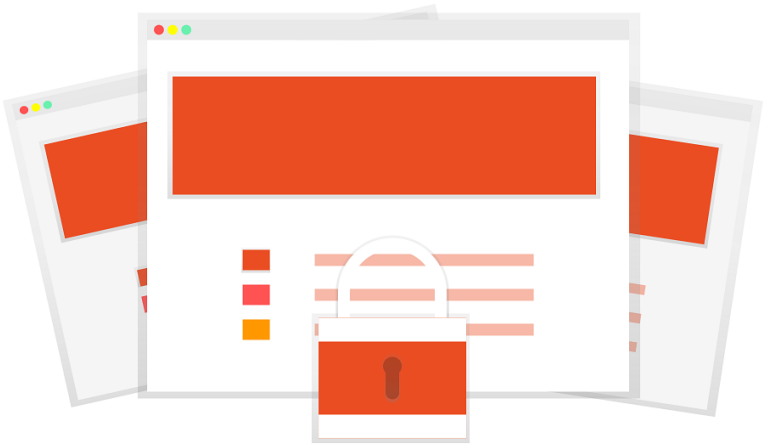
Den menneskelige faktor i IT-sikkerhed

Undersøgelse af IT-sikkerhed med fokus på den menneskelige faktors involvering og hvordan sikkerhedsforanstaltninger kommunikeres succesfuldt til medarbejdere. Præsenteret i samarbejde med COWI.



COWI

Lasse Jakobsen

Sylvester Faurschou

Daniel Nørby Nielsen

Lasse Rehder Sørensen

Simon Eliasen

Faculty of Computer Science
Aalborg University
Denmark
19/12/2019

AALBORG UNIVERSITY
DENMARK

Andet Studieår v/ Informationsteknologi og Informatik
CREATE
Rendsburggade 14
9000 Aalborg
http://www.aau.dk

Titel:

Den menneskelige faktor i IT-sikkerhed

Projekt:

Kommunikation og Organisationer

Projektperiode:

September 2019 - December 2019

Projektgruppe:

Projektgruppe 3

Deltagere:

Lasse Rehder Sørensen
Simon Eliasen
Daniel Nørby Nielsen
Lasse Jakobsen
Sylvester Faurschou

Vejleder:

Pirkko Liisa Raudaskoski

Abstract

This paper seeks to examine the strategic communication regarding the use of IT-courses in an organization as a way of educating the employees in best practices regarding IT-security. This arise from the larger problem regarding the majority of security risks in modern IT-systems being human error.
Furthermore the paper seeks to uncover how the employees at COWI view the IT-courses' with an emphasis on the challenges that arise from the courses and the employees' attitudes towards them.

Sidetal: 130
Appendiks: 71
Afsluttet 19-12-2019

Forord

I led med 3. semesters projekt på Aalborg Universitet, med fokus på strategisk kommunikation og organisationer, er følgende rapport udarbejdet af fire studerende på bacheloren i informationsteknologi og en studerende på informatik.

Vi vil gerne rette en stor tak til vores vejleder, Pirkko Liisa Raudaskoski, for at have leveret fantastisk dog udfordrende feedback for studerende fra et naturvidenskabeligt studie. Ydermere vil vi gerne rette en tak til COWI for at lade os interviewe deres ansatte såvel som ledelse, i egne lokaler. Vi takker især for åbenheden inden for et emne, som ellers normalt ikke er så let tilgængeligt.

Læsevejledning

Formattet for kildeangivelser i teksten er (forfatter, år) og henviser til litteraturlisten, som findes til sidst i rapporten før bilagene, hvor informationer om kilderne er uddybet.

Figurer og modeller vil blive nummereret i forhold til, hvilket kapitel de findes eksempelvis *4.1*. Under hver enkelt figur forekommer en beskrivelse til den givne figur. Når der jævnføres til forhenværende afsnit og bilag, skrives det henholdsvis (J.f (afsnit)) og (J.f bilag). I analysen refererer vi til transskriberingen, som skrives (J.f bilag:x), hvor x henviser til nummeret for den specifikke udtalelse.

Skrives der *vi* eller *vores* i rapporten, vil det referere til projektgruppen.

For at mindske informationerne tabt i en oversættelse af fagtermer, vælges der at skrive disse på deres originale sprog, hvis termerne bærer specifik fagterminologi.

Indholdsfortegnelse

Tematisk redegørelse 1

Den tematiske opsætning er udarbejdet fra den angivne studieordning for 3. semester på Informationsteknologi og Informatik. Heri er semestrets centrale omdrejningspunkt angivet som: 'Strategisk kommunikation og organisationer', afledt af projektfaget med samme navn. Semester rammen for projektet lyder som følgende „strategisk kommunikation med fokus på kommunikation i og fra organisationer (Universitet, 2015).“ Projektet tager afsæt i den strategiske kommunikation, der foregår internt i virksomheden COWI, hvor der tages udgangspunkt i interviewempiri. Denne form for strategisk kommunikation er interessant at analysere, da samfundsbilledet er præget af øgede IT-trusler. Projektet undersøger COWIs intentioner vedrørende IT-sikkerhed samt medarbejdernes holdninger til de indførte IT-sikkerhedskurser. For en gennemarbejdet analyse bruges der teorier om strategisk kommunikation og organisationsteori, da dette også er en essentiel del af studieordningen.

Problemanalyse 2

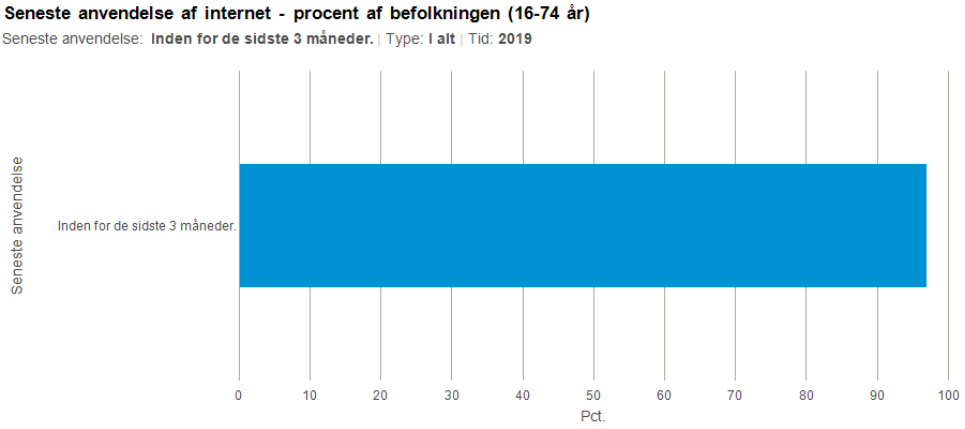
2.1 Indledning

IT er en central del af vores dagligdag. Vi bruger IT til at tjekke vores bankkonti, modtage beskeder fra regeringen og handle online. Trods den store bekvemmelighed ved disse services, opstår der markante problemer, når først en af disse svigter. Der kan især perspektiveres til menneskets integrerering med teknologien, som øges ved hjælp af mobile enheder, wearables og sågar et løfte om fremtidige IT-implantater. Vi må erkende, at vi i dagens Danmark ikke blot skal værne os fysisk og psykisk, men i høj grad også digitalt. Heraf må vi forsøge at afmystificere de skjulte lag af digital sikkerhed, som i højere grad virker læslig for maskiner end for mennesker. Dette er sandsynligvis overkommeligt for IT-kompetente brugere, men hvordan formår nogle som eksempelvis en hel organisation, at varetage et system der betragtes som værende sikkert?

2.2 Problemfelt

Med det overvældende fokus på sikring af IT-systemer i moderne litteratur (Borre, 2017) (Marcus, 2018) (Kristine Holst, 2018), vil vi fokusere på den menneskelige faktor og dens sammenspil i sikkerhedsbrud. Mere konkret hvordan moderne organisationer værner sig mod digitale angreb.

97% af danskere havde i 2019 brugt internettet inden for de seneste 3 måneder, som set i figur 2.1 (Statestik Universitet, 2018). Tal fra 2008 viser også at 98% af virksomheder havde internetadgang (Statistik, 2015). Det kan derfor udledes at IT har en central rolle både privat såvel som i virksomheder. Tal fra Danmarks Statistik understøtter ligeledes det stigende antal af virksomheder, hvor IT er en central del af virksomhedens kerneydelser (Statistik, 2017).



Figur 2.1. 97% af danskerne har været på internettet inden for de seneste 3 måneder(Statestik Universitet, 2018)

Gordon Moores lov dikterer at vi hvert år kan se en fordobling af antallet af transistorer, der kan placeres på en mikrochip (Moore, 1998). Dette korrelere til den økonomiske teori om udbud og efterspørgsel, hvor et højt udbud af enkelte transistorer fører til mindre omkostninger af computerkraft. Der er flere konsekvenser af Moores lov, såsom øget kompleksitet af software, størrelsen af softwareapplikationer (Wirth, 1995) og en tendens til at software bliver forældet hurtigere (Sandborn, 2008). Det øgede antal af forældet software fører til lavere indgangsbarrierer for uhensigtsmæssig indtrængere, hvilket også medfører et øget fokus på IT-sikkerhed i organisationer (Statistik, 2015). Hertil må organisationer konstant udvikle mere komplekse systemer, for at holde uhensigtsmæssige indtrængere i skak.

Når der i daglig tale snakkes om IT-sikkerhed, kan der være en tendens til at snakke om sikkerheden af softwaren som computere benytter. Nye tal viser dog, at den største faktor for brud på IT-sikkerhed er menneskelig, og at 52% af sikkerhedsbrud er grundet human error (CompTIA, 2015). Dette kan sandsynligvis skyldes den øgede kompleksitet som Moores lov dikterer. Når vi i denne kontekst snakker om human error, så er det primært phishing angreb vi bekymrer os om, hvor hackere søger at *fiske* informationer fra brugeren. Dette kan få en organisation i et jerngreb, hvor de kan eksponeres for såkaldt ransomware, hvor organisationers filer holdes som gidsel. Her bliver organisationen afpresset til at betale løsepenge for at genvinde adgangen til deres IT-systemer (sikkerdigital.dk, 2019). Disse phishing angrebs kompleksitet og antallet af dem er i høj grad stigende (Danmark Statistik, 2019), hvor det blandt andet ses at uhensigtsmæssige indtrængere udgiver sig for at være ens chef, enten pr. e-mail (TV2, 2019) eller telefonopkald (Web, 2019). Derfor er organisationer nødt til at indsætte sikkerhedsprocedurer for at undgå brud på deres IT-systemer.

2.2.1 Strategisk Kommunikation

Opgavens omdrejningspunkt vil være at analysere den strategiske kommunikation. Definitionen herpå udeledes fra Kirk Hallahans *„Defining strategic Communication“*, hvori strategisk kommunikation beskrives som *„the purposeful use of communication by an organization to fulfill its mission“* (Hallahan, Derina Holtzhausen, Betteke van Ruler, Dejan Verčič, & Krishnamurthy Sriramesh, 2015, s. 3). Den strategiske kommunikation kan komme igennem administrative procedurer, hvor kommunikationen skal sikre overførelsen af information fra leder til medarbejder, for at skabe føjelighed samt sikre virksomhedens position i samfundet (Hallahan et al., 2015).

Hallahan opstiller seks overordnede områder inden for strategisk kommunikation: *management communication, marketing communication, public relations, technical communications, political communication og information/social marketing campaigns* Hallahan et al. (2015). I dette projekt tages der udgangspunkt i *technical communications*, for at se på hvordan medarbejdere undervises i IT-sikkerhed i organisationen, hvordan dette er modtaget af medarbejderne og hvilke udfordringer dette leder til.

2.3 Problemformulering

På baggrund af ovenstående afsnit har projektgruppen udarbejdet følgende problemformulering:

Hvad er COWIs medarbejderes holdninger til deres nuværende IT-kurser, og hvilke udfordringer har disse IT-kurser medført?

2.4 Videnskabsteoretisk standpunkt

Den videnskabelige tilgang „etnometodologi“ tager afsæt i fænomenologien. Den grundlæggende forskel er dog at i stedet for at koncentrere sig om den individuelle fortolkning, interesserer etnometodologien sig for den offentlige dimension i betydningsdannelsen (Raudaskoski & Paul McIlvenny, 2013). Harold Garfinkel, grundlæggeren af etnometodologien, har opstillet en liste som beskriver etnometodologiens undersøgelses policer. Listen består af:

1. Ethvert term, koncept, kategori aktivitet er defineret af deres situationelle brug. De er ikke forståelige uden for konteksten af deres brug. Dette kaldes den indeksikalske handling.
2. Mennesker er i stand til at tolke situationen de står i, selvom ord og handlinger er indeksikalske. Dette er handlingers praktiske natur.
3. Handlinger kan ses som en selvreferentiel proces hvor ord og handlinger danner grundlag for videre handling som stabilisere den tidligere. Det er ikke muligt at forstå en handling uden dens kontekst og vice versa. Konteksten bliver dannet i handlingssituationen (Koskinen, 2000b).

Etnometodologien ser mennesket som værende ræssoneret, opmærksom og fuldfører opgaver i deres givne kontekst. Hvis en observerbar handling afviger fra andres skal handlingen argumenteres eller korrigeres. Dette beskrives af Garfinkel som værende handlingsansvar. Det er ikke bare den sociale kontrol, der er på højkant, men vores tillid til at handle korrekt. Handlinger er gennemgribende refleksive, hvilket ifølge Lucy Suchman betyder at de er situerede. Dette vil blive forklaret yderligere i afsnit 5.4.2 (Koskinen, 2000b).

Ifølge Ilpo Koskinen er menneskelige handlinger ikke skrøbelige, men robuste. Dette er grundet at mennesker strukturerer handlinger ud fra etnometodologier, hvilke varierer i forhold til situationen. En af de primære handlinger er *institutional interaction* som er interaktion, der orienterer sig mod at opnå et givent institutionelt mål. I de fleste tilfælde er institutionel interaktion organiserede spørgsmål stillet af en professionel og svarene givet af klienten (Koskinen, 2000b).

I dette projekt ses der på COWIs strategiske kommunikation vedrørende sikring af IT-sikkerheden gennem IT-kurser. Analysenmetoden anvendt til dette er en etnometode, nemlig en interaktionsanalyse. Dette vil blive uddybet i afsnit 5.4.3.

Casebeskrivelse af COWI 3

Til besvarelsen af problemformuleringen har vi indgået et samarbejde med COWI. Her vil vi i det følgende kapitel undersøge organisationens interne og eksterne faktorer, som kan have påvirkning på deres strategiske muligheder. Denne udarbejdelse vil ydermere have relevans i udarbejdelsen af senere analysearbejde, hvori en øget viden, kan bidrage til en dybere forståelse for personernes individuelle handlerum, og sågar organisationens. Empirien i kapitlet tager udgangspunkt i et interview med COWIs Chief Information Manager (CIO) (J.f G), som er IT-ansvarlig og står for IT-sikkerheden. Yderligere data er indsamlet fra organisationens hjemmeside (COWI, 2019b), såvel som deres årsrapport (COWI, 2019c).

3.0.1 Virksomhedsbeskrivelse

COWI er en førende rådgivningsvirksomhed, med ekspertise inden for ingeniørkunst, miljø og samfundsøkonomi. De forsøger at takle udfordringer fra mange forskellige vinkler, for at skabe mere sammenhængende løsninger for deres kunder. Med kontorer over hele verden, har de en global tilstedeværelse og løser projekter i hele verden – store såvel som små. COWI har på ethvert tidspunkt gang i mere end 14.000 projekter. De har over 85 års erfaring i rådgivningsbranchen, og med 7.300 medarbejdere er de store inden for deres felt. COWIs nuværende driftsresultat er på 283 millioner kroner med en omsætning på 190 millioner kroner. Begge har set høj vækst siden 2015. COWIs vision er at være en topspiller i industrien, kundens første valg, have de bedste medarbejdere, være et ledende brand, have verdensklasse internationale specialister og have fremragende resultater.

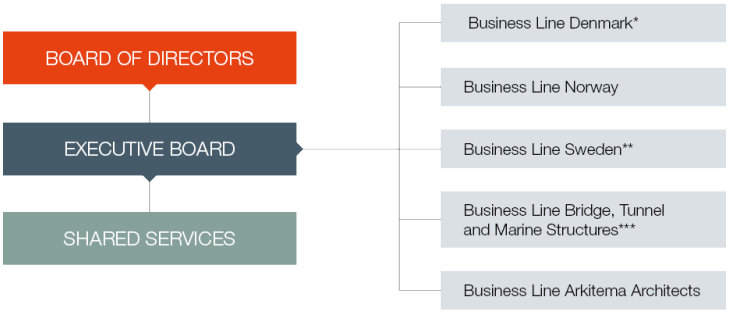
COWIs mission og eksistensgrundlag er at skabe signifikant værdi for deres kunder, mennesker og samfundet, igennem viden og en 360° tilgang ved at involvere og engagere kunder og stakeholders i samarbejde, der fører til optimale løsninger, anvendelse af førsteklasses viden og erfaring globalt såvel som lokalt, baseret på ingeniørkunst, økonomi og miljøvidenskab samt at skabe velstand og muligheder for kunder, ansatte, shareholders og andre stakeholders.

3.0.2 COWI og IT-sikkerhed

COWI har i nyere tid opgraderet sin sikkerhed i kampen mod cyberkriminalitet, heriblandt ved hjælp af en ISO 27001 sikkerhedscertificering (*COWI opgraderer it-sikkerheden*, 2019). COWI bruger på nuværende tidspunkt, i relation til rapportens problemfelt, IT-sikkerhedskurser til at informere deres ansatte om nye trusler de skal være opmærksomme på. Undervisningsmaterialet er tilgængeligt for de ansatte på COWIs interne portal, og har en tidsfrist for gennemførelse. Vigtigheden af implementering af IT-sikkerhed hos COWI er primært manifesteret i at de lever af at sælge timer. Hvert systemnedbrud, der gør folk uproduktive, koster penge, hvilket er hovedgrundlaget for deres interesse i optimering af IT-sikkerhed.

3.0.3 Organisationsstruktur

COWI er opbygget som en hierarkisk organisation, hvor der er klar opdeling af ledelse og mening medarbejder. Ledelsesstrukturen er dog decentraliseret, da der findes projektkontorere spredt ud over verdenen.



Figur 3.1. COWIs organisationstruktur (*COWI organisationsstruktur*, 2019)

Som opsummeret i figur 3.1 ses COWIs organisationsstruktur, som viser en primær ledelse, med en bestyrelse. Den resterende del af organisationen er opdelt i afdelinger, som enten er opdelt pr. funktion eller geografi.

Under bestyrelsen og direktørerne, er der dernæst executive presidents, som står for en overordnet afdeling såsom Danmarks-afdelingen. Herunder er der senior vice presidents, som står for overordnede områder eksempelvis miljø. Derefter er der vice presidents, der står for afdelinger i miljø-området eksempelvis, og til sidst er der den almene medarbejder. Herudover er der også en række medarbejdere, som arbejder uden for denne organisationsstruktur i et vist omfang. Disse medarbejdere er spredt på projektkontorer udover hele verdenen.

Med henblik på organisationsstrukturen er der en klar opdeling af arbejdsopgaver relateret til forskellige styringniveauer. Her står ledelsen for de overordnede strategiske beslutninger, hvoraf det er de resterende ansatte der skal efterleve disse beslutninger, såsom implementeringen af IT-sikkerhedskurser.

3.0.4 Morgans organisationsmetaforer

Med udgangspunkt i COWIs virksomhedsbeskrivelse, redegørelsen for aktiviteter i henhold til IT og beskrivelsen af deres organisationsstruktur, vil vi klassificere COWI ud fra Morgans organisationsmetaforer. Her vil vi ved hjælp af repræsentative metaforer mindske kompleksiteten, når vi snakker om noget så komplekst som en organisation.

Morgan forklarer i teorien om organisationsmetforer, at den måde vi forstår og definerer en organisation på, afhænger af det mentale billede vi har af denne; „most definitions and theories of organization can be associated with a particular organizational methapfor“ (Jaffee, 2000, s. 6). Som der ses af citatet ovenover foreslår Morgan benyttelsen af organisationsmetaforer for at øge forståelsen af organisationeners kompleksitet.

COWI kan forbindes med organismemetaforen, som sammenlignes med en levende organisme, da det er en altid ændrende struktur, der har brug for en konstant strøm af ressourcer for at fungere, og med tiden vokse. Ud fra dette perspektiv fokuseres der også på en organisations konkurrenceevne, da den er altafgørende for dens fortsatte vækst, og hermed overlevelse.

COWI har som sagt en målsætning om at være en topspiller inden for industrien, der ved at skabe signifikant værdi for deres kunder, mennesker og samfundet, vil indtage positionen som kundernes foretrukne valg. I og med COWI befinder sig i en konkurrencepræget branche, kræver det at organisationen tilpasser sig miljøet, for fortsat at kunne yde deres bedste. COWI kan også henvises til denne metafor i forhold til ledelsesstrukturen. Som nævnt i (j.f 3.0.3), består COWI af en overordnet ledelse, hvorunder organisationen er opdelt i afdelinger. Dette passer med det mentale billede af COWI som en organisme, da der her er en forventning om at ledelsen kommunikerer og formulerer planer og beslutninger til afdelingerne som respons på miljø-/branchemæssige ændringer, som COWI som organisme skal forholde sig til.

3.1 Virksomhedsøkonomisk analyse af COWI

På baggrund af den indsamlede empiri i led med casebeskrivelsen, vil vi tage et virksomhedsøkonomisk perspektiv på COWI som virksomhed. Heri undersøges den kontekst COWI indgår i, både i led med de eksterne omgivelser samt de interne forhold, som har indflydelse på COWIs strategiske plan i forhold til IT-sikkerhed. Mere specifikt så vil vi analysere og forstå deres nuværende tilgang dertil. De interne forhold vil uddrages fra tidligere afsnit. Ydermere vil de eksterne forhold opsættes i en PEST-analyse. Ud fra disse kan vi kategorisere interne styrker og svagheder samt eksterne muligheder og trusler. Det vil give os input til en SWOT-analyse, der kategoriserer COWIs handlerum, og eventuel incitament, for deres nuværende handleplan. Kort sagt vil SWOT-analysen hjælpe os med at identificere strategiske muligheder, som COWI kan udnytte ved at gøre brug af eksterne muligheder, modstå trusler, bygge eller beskytte styrker og bekæmpe svagheder.

3.1.1 PEST-analyse

PEST-analysen vil bruges til at identificere eksterne faktorer, som påvirker organisationens handlerum. Dette resultat kan bidrage til identificering af eksterne trusler og muligheder. Disse kan vi senere kombinere med interne faktorer, for derefter at anvende dem i en SWOT-analyse, hvor vi kan give et bud på strategiske muligheder derfra (Clulow, 2005).

Political ser på i hvor høj en grad det politiske landskab har påvirkning på den specifikke virksomhed. Det kan eksempelvis være lovgivning vedrørende skat, import, eksport og miljø eller eventuelt et ustabilt politisk system. **Economic** er den nuværende økonomi og dens performance nationalt, såvel som internationalt. Det kan være elementer såsom lavkonjunktur, et lavt rente niveau og andre lignenede faktorer, som påvirker virksomhedens drift. **Social** er ting såsom demografiske forhold, uddannelsesniveauet og indkomstfordelingen. Alle disse faktorer undersøges for at forstå strategivalget overfor den givne befolkning, og ultimativt forstå brugeren og det miljø der ageres i. **Technological** beskæftiger sig med den anvendte teknologi i branchen. Det kan være om den nyeste teknologi benyttes. Dette kan bruges med stor fordel til at styrke virksomhedens position, men kan omvendt også medføre forældet software, som påvirker konkurrencen i virksomheden (Clulow, 2005).

Political

Med henblik på politiske faktorer, som kan have påvirkning på COWIs virke, er der som udgangspunkt krav om at overholde lovgivning i led med bogføring, og overholdning af

kontraktarbejde med det offentlige såvel som det private. Herudover er der også internationale faktorer, såsom USA og Kinas handelskrise og Brexit forhandlinger, som kan have en indvirkning, grundet COWIs internationale råderum. Her er den internationale konkurrence også vigtig, da den ligger et konstant pres på innovation internt i virksomheden.

Economic

Som nævnt i politiske faktorer har international politisk usikkerhed påvirkning på det økonomiske resultat. I nyere tid er det primært Brexit og Kina-USA handelskrisen, som er steder hvor COWI har repræsentanter eller arbejdsopgaver. Det internationale arbejde sætter også krav om en forståelse for det økonomiske billede, hvor aktiver haves i led med et svingende marked, og ydermere beskatning internationalt.

Social

COWIs primære produkt er konsulenttimer. Derfor stilles der et massivt krav til at behandle medarbejderne godt, både for at sikre sig god omtale og for at opnå bedre resultater. Kulturelle faktorer er også vigtig at medtænke, hvor traditioner og skikke varierer i høj grad i lande hvor COWI har medarbejdere, samarbejdspartnere og kunder. Eksternt ligger der i høj grad også et pres med hensyn til virksomhedens Corporate Social Responsibility (CSR), hvor en moderne virksomhed kræves at have et lavt miljømæssigt aftryk, overvejelser og omtanke i forhold til diversifikation med henblik på inkludering af minoriteter. Yderligere er forholdsregler i forhold til korruption og arbejdsmiljø også vigtigt.

Technology

Inden for IT er GDPR (Persondataforordningen) et stort emne i nyere tid. Dette øger kompleksiteten af kommunikation, hvor flere tilladelser skal indhentes, og et øget fokus herpå er derfor krævet, for at overholde den europæiske lovgivning. Eksternt lægges der også et fokus på at COWI skal have robuste IT-systemer, da systemnedbrud i en virksomhed, der i så høj grad er digitaliseret, kunne udmunde i tab på op til flere millioner kroner. Dette ville både svække deres omdømme, såvel som mindske troværdigheden til dem i et internationalt marked med høj konkurrence. Her er det også vigtigt at have robuste systemer til international kommunikation, som sikre at arbejdsopgaver ikke er hindret af dårlige redskaber. I led med samarbejdspartnere som forsvaret og atomkraftværker er det også vigtigt for dem at have såkaldte *black boxes* der sikrer yderst fortrolig kommunikation, der sikrer at data bliver behandlet med yderst fortrolighed, inden for strengere retningslinjer. COWI må som virksomhed også reagere på konstant udviklende teknologier, som markedsleder på flere miljørelaterede konsulentydelser, og sikre sig at de i høj grad bibeholder denne titel, og ikke bliver efterladt i gamle teknologier. Gamle teknologier kan også i nogle kontekster, betyde øget eksponering overfor hacking, hvor uhensigtsmæssige indtrængeres redskaber lader til at stige parralelt med virksomheders foranstaltninger.

3.1.2 SWOT-analyse

På baggrund af analysearbejdet foretaget i led med PEST-analysen og empiri fra casebeskrivelsen, vil vi henholdsvis uddybe styrker og svagheder i led med de interne forhold. Dernæst vil vi kategorisere de eksterne forhold, ved hjælp af muligheder og trusler fra PEST-analysen.

Dette gøres med formålet om at få en overordnet indsigt i COWI og de bagvedliggende faktorer, som ligger til grund for deres strategiske planlægning. Dette vil give en øget forståelse for den nødvendige baggrundsviden til succesfuldt analysearbejde og klassificering af COWI som organisation. Dette vil føre til et bud på strategiske muligheder, i led med det identificerede SWOT indhold.

Styrker

En af de primære styrker ved COWI er deres højtuddannede arbejdskraft. Dette udmunder også i et højt fokus på menneskelige ressourcer. COWI er markedsleder i flere felter relateret til miljø. virksomhedens aktier er ejet af medarbejdere og COWI, og kan derved motivere medarbejdere yderligere derigennem. COWIs omsætning er stigende, hvilket giver dem god rådighed på markedet. Det gør at de har råd til at investere markant i IT-sikkerhed, hvor alle fastansatte er pålagt at deltage, ved hjælp af deres online platform, COWI-academy. Dette er altsammen yderligere tiltag end hvad der kræves lovmæssigt, hvor COWI er ledende inden for investering i IT-sikkerhed i deres branche, heriblandt ved implementering af en ISO 27001 certificering, selvom de ikke er et umiddelbart mål for hacking. Til sidst er der også et højt fokus, med oprindelse i eksterne forespørgsler, heriblandt foranstaltninger inden for CSR (COWI, 2019a), diversitet, investering i miljø og anti-korruption.

Svagheder

Svagheder forbundet med COWI kan være at deres primære produkt som servicevirksomhed er konsulenttimer. Derved kræver det utroligt mange ressourcer at udbyde et IT-kursus, da et 30 minutters kursus, skal ganges med omtrent 7300 medarbejdere. Herudover er det kun de fastansatte, der modtager kurserne, som potentielt kan eksponere eksempelvis praktikanter, deltidsansatte eller studentermedarbejdere. Medarbejdere i COWI er også delt ud over verden. Derfor er der ikke en reel opfølgning på, at alle afgrene af virksomheden følger de angivne krav og retningslinjer.

Muligheder

COWI er en allerede veletableret virksomhed, der med en lang historie har etableret sig som et succesfuldt brand. Her har de valgt et fokus på deres omverden og hvad der bevæger sig heri. COWI har allerede vundet stor succes med etablering af IT-sikkerhedsforanstaltninger, især i højere grad end hvad der er forventet af deres industri. Dette er også evident i deres valg om at anskaffe sig en ISO 27001 sikkerhedscertificering, heri kan denne med fordel benyttes i led med den samfundsmæssige efterspørgsel af IT-sikkerhed i organisationer. COWIs fokus på teknologi, ses også i troværdigheden de har opbygget, hvilket resulterer i kontraktarbejde for forsvaret såvel som for atomkraftværker. Dette manifesterer sig også i deres allerede etablerede foranstaltninger i led med GDPR, og deres omfattende Corporate Social Responsibility (CSR), der blandt andet søger øget diversitet, antikorruption og miljøvenlighed. Alle disse store eksterne efterspørgelser er noget COWI i høj grad kan kapitalisere på, grundet deres nuværende etablering og foranstaltninger inden for emnefelterne.

Trusler

De eksisterende trusler, generelt såvel som i COWI, er den konstante kamp om at være på forkant med hackere, hvor udviklingen som førnævnt stiger lineært på begge sider. Her er det ydemere prisen ved et sådant angreb, der kan være bekymrende for en virksomhed, der er digitaliseret i så høj grad. Det at være international kommer også med udfordringer. Der er høj konkurrence, som kræver konstant innovation og optimering fra COWIs side. Det internationale politiske miljø kan også påvirke virksomhedens virke. Her kan økonomiske udsving blandt andet have stor indvirkning, hvis mange aktiver eksempelvis er placeret i et land. Det politiske landskab kan også i høj grad påvirke COWI, eksempelvis er der her i nyere tid handelskrigen mellem Kina og USA, såvel som Brexit. Hvis vi fokuserer på COWIs nuværende IT-kurser specifikt, er der også en høj omkostning forbundet herved. Indkøb af licenser hertil er utrolig dyrt i så stor en virksomhed. Her kan der også yderligere tilføjes usikkerheden ved at have eksterne udbydere af kurser, hvor en tidligere udbyder allerede har været fravalgt, grundet manglende kvalitet. I den forstand kan der siges, at COWI ikke er i fuldkommen kontrol over indlæring af sikkerhed hos deres egne medarbejdere, grundet brug af en ekstern udbyder af kurserne.

Strategiske muligheder

Fra overstående analyse ses det at COWIs fokus på IT-sikkerhed er af høj kaliber. Dette er blandt andet synligt ved implementeringen af ISO 27001 certificeringen, som stiller krav til implementering af et informationssikkerhedsledelsessystem og vedligeholdelse deraf. COWI er yderligere vant til håndtering af højprioritets kunder såsom det danske forsvar og atomkraftværker, og har etableret krypteringsteknologi, der lader dem arbejde i såkaldte *black boxes*. Kort sagt er de etablerede IT-systemer yderst tilfredstillende, sammenlignet med deres branche. Dette er yderligere set i lyset af at de umiddelbart kun bliver udsat for hacking, der er af opportunistisk affart.

Selvom de implementerede IT-systemer er af høj standard, er det dog vigtig at se på de menneskelige ressourcer, og deres medspil i eventuelle brud på sikkerheden. Dette er især set i lyset af at primære sikkerhedsbrud er muliggjort via menneskelige fejl, ved hjælp af metoder såsom social engineering (CompTIA, 2015). Ud fra denne viden ville det være fordelagtigt for COWI at fokusere på den risiko deres medarbejdere udgør, og se på hvordan dette kunne mindskes. Dette er essentielt da COWI som førnævnt, i høj grad er en digitaliseret virksomhed, som udbyder services, der i et højt omfang er afhængige af online IT-teknologier, hvor et systemnedbrud kan have en markant økonomisk indvirkning på virksomheden, eller deres troværdighed som internationale markedsledere.

Ud fra dette vil vi i denne rapport søge at analysere de udbudte IT-kurser fra COWI for at identificere fejl og mangler, såvel som styrker. Dette gøres for at få et yderligere indblik i, hvordan den menneskelige faktor og dens tilsyneladende risiko kan mindskes, og om kvaliteten af disse kurser, er af lige så høj standard som deres IT-systemer.

Denne strategiske mulighed tager udgangspunkt i COWIs etablerede styrke inden for deres sikre IT-infrastruktur og kommunikationskanaler og søger at mindske og undvige truslen om menneskelige fejl og store tab ved nedbrud af systemer. Dette er er en såkaldt ST-strategisk mulighed, som tager udgangspunkt i at minimere trusler for virksomheden, ved at udnytte deres styrker.

Teori 4

I følgende kapitel vil de anvendte teorier blive gennemgået. Der er her tale om David Jaffees teorier om *tension and change* i en organisation. Dette vil blive efterfulgt af Beverly Burris' teori om *computerizations* og dennes indflydelse på organisationen. Dette inkluderer struktur, teknologiens indvirkning på arbejdsstyrken og hvordan teknologien er med til at omstrukturere virksomheden. Foruden disse vil Davide Nicolinis teorier om *zooming in* og *zooming out* blive redegjort for. Dette er for at skabe bro mellem teori og analyse.

4.1 Jaffee's analyseramme for organisationskommunikation

Jaffe fremlægger en konceptuel ramme for analyse af organisationskommunikation(Jaffee, 2000). Her fokuseres der på to paradigmer: det intraorganisationelle og interorganisationelle niveau. Heri kan vi i led med rapporten, med udgangspunkt i det intraorganisationelle niveau, analysere udfordringer som ville kunne opstå i led med de anvendte IT-kurser.

Når der tales om det **intraoganisatonelle niveau** er det orienteret imod den interne organisationskultur. Her er der tale om formel og uformel interaktion mellem medarbejdere, den organisatoriske kultur, organisationens strukturelle design og metoder af organisatorisk kontrol, som kan forekomme i organisationen.

Det **interorganisationelle niveau** retter sig mod ekstern interaktion til andre organisationer eller til deres omverden. Her kan der eksempelvis være tale om leverandører, markedet, kunder og regeringen.

Overordnet vil en fyldestgørende analyse af en organisation både analysere det intraorganisationelle og interorganisationelle niveau. Det vil give et større samlet indblik i organisationen og dens virke.

Jaffe omtaler også **transaktioner**. Her er der helt konkret tale om det mest centrale element i organisationen, altså overlevering af varer, eksempelvis fra udbyder til modtager. Her kan der både være tale om produkt eller service. Fra dette udspringer der dog også to essentielle problemstillinger eller såkaldte **tensions**, som skal balanceres nøje for at opnå balance i en virksomhed.

Tension 1: Den menneskelige faktor Den menneskelige faktor beskriver forholdet mellem den ansatte og organisationen. Mennesket, set som ressource, er unik i sin refleksive og reaktive natur, hvoraf der kan observeres, evalueres og reflekteres overfor organisationelle forhold. Dette gør ofte etableret teori til skamme grundet uforudsigeligheden, og udgør en af de største udfordringer ved organisationsteori og management praksisser. Herunder skal der tages forbehold for menneskets forskelligheder grundet deres forskellige baggrunde og yderligere

at deres job udelukkende er en lille refleksion af dem som person, som ikke tager højde for personlig baggage og særheder.

Tension 2: Balancering af differentiering og integrering Med henblik på at finde en balance mellem differentiering og integrering, ses der på det intraorganisationelle niveau på differentiering, som værende en teknisk opdeling af arbejdskraft, såsom forskellige opgaver, beskæftigelser og afdelinger. Her ses integrering som værende social integrering, herunder integration af mennesker gennem kommunikation, interaktion og kultur. Ses der på differentiering i det interorganisationelle niveau er der fokus på social opdeling af arbejdskraft som forskellige virksomheder, produktion, leverandører og distributører, og i forhold til integrering er der fokus på funktionel integrering. Dette betyder integration af organisationelle enheder, som er involveret i stadier af produktion og distributions processen.

4.2 Beverly burris' opdeling af organisatoriske omstruktureringer ved implementering af teknologi

Beverly Burris bevæger sig, ligesom David Jaffee, inden for organisatoriske omstruktureringer på baggrund af forskellige faktorer. Burris arbejder inden for hvad Jaffee ville kategorisere som det intraorganisationelle niveau, men hun har udvidet med teorien om hvad implementeringen af teknologi gør ved interaktionen af de forskellige fokuspunkter i Jafees teori (j.f 4.1). Dette er en relevant teori at bruge, til at danne et grundlag for besvarelsen af hvordan indførslen af e-kurserne har ændret medarbejdernes opfattelse af IT-sikkerhed.

4.2.1 Organsationsstruktur

Burris mener at *computerization* har en korrelation med færre hierarkiske niveauer inden for en organisation. Dette står i kontrast til specialiseret arbejde, hvor der er en mere klar kommandostruktur. De færre hierarkiske niveauer betyder at midterpositionerne er reduceret eller elimineret, hvor det eneste der adskiller de øvre niveauer fra de nedre, er højere uddannelse eller anbefalinger (Burris, 1998).

Restruktureringen af organisationen er afhængig af flere faktorer: den specifikke type af teknologi, ledelsesmæssige policer og valg samt servicen eller produktet som bliver leveret af firmaet. Hvis produktionen af enten servicen eller produktet kan standardiseres og udføres af et computeriseret system, vil organisationen i højere grad bestå af kompetente tekniske arbejdere, og et mindre antal af produktions- og kontormedarbejdere. Jo mere computeriseret en organisation er jo færre produktionsmedarbejder findes der i organisationen. Hvis ikke det er muligt at standardisere den service eller de produkter organisationerne leverer, mener Burris at polariseringen af arbejdsstyrken ikke vil være lige så fremtræden (Burris, 1998).

Konsekvenser ved polarisering

Der er opstillet nogle logiske konsekvenser associeret med polariseringen. Den første hun beskriver, er at organisationsstrukturen bliver mindre formel. Computeriserede organisationer gør mere brug af ad hoc teams og arbejdsgrupper.
Den anden konsekvens som Burris opstiller, er at interne arbejdsmarkeder nedbrydes. Med det menes der, at organisationer hellere søger arbejdere med anbefalinger andetstedsfra eller

konsulenter, i stedet for interne oplæringer og forfremmelser.
Den sidste logiske konsekvens ved polariseringen er, at der sker en forstærkelse af opdelingen i race og køn i nogle organisationer (Burris, 1998).

4.2.2 Teknologiens indvirkning på centralisering og decentralisering

Burris beskriver hvordan sociale og politiske valg interagerer med teknologiske overvejelser, som danner forskellige former for centralisering og decentralisering. Det opstilles som to aspekter hvor den ene søger at strømline og effektivisere operationen, og den anden omhandler mennesker og deres relation til hinanden og teknologien. Det første aspekt kommer primært til udtryk som værende en del af en centraliseret organisation, hvor kulturen peger på ordre og kontrol. Det andet aspekt er en del af en mere decentraliseret organisation, hvor medarbejderne har indflydelse på deres egen praksis.
Ved implementeringen af ny teknologi sker der enten en assimilering hvor teknologien falder i med organisationsstrukturen, eller en akkomomdation hvor teknologien omstrukturerer organisationen. Der har været en tendens til at teknologi, der stemmer overens med en centraliseret struktur, kan lede til spændinger, faldende tilfredshed blandt medarbejdere og skabe yderligere forandring i organisationen (Burris, 1998).

4.3 Nicolini - Et blik på situationer som praksis

Nicolini har i sin rapport „Zooming In and Out: Studying Practices by Switching Theoretical Lenses and Trailing Connections“ fokus på at undersøge arbejdssituationer i praksis, ved at zoome ind og ud på den lokale praksis igennem teoretiske og metodiske linser. Her har han særlig interesse i, at undersøge fænomener inden for organisationelle studier. Målet med rapporten er derfor at skabe nogle rammer for at studere, analysere og repræsentere praksisser. Teorien er relevant for rapporten, da den beskriver den gennemgående praksis ved først at starte med at zoome ud, hvilket i denne kontekst beskrives ved anvendte teori og metoder, for derefter at zoome ind i den konkrete kontekst og praksis i form af interaktion- og indholdsanalyse. Til sidst zoomes der ud i et bredere perspektiv i led med den afsluttende diskussion, perspektivering, konklusion og eventuelle løsningsforslag.

I Nicolinis *zooming in* introduceres et antal af konceptuelle værktøjer som hjælper forståelsen af praksisser. Af hensyn til rapporten og for at bevare overblikket, er kun de relevante perspektiver udvalgt her, og det er derfor kun disse der beskrives. I analysen er der valgt at zoome ind på den lokale praksis, ved at se på hvad der bliver sagt og gjort, ud fra et etnometodologisk perspektiv. Her undersøges den indsamlede empiri nærmere igennem en interaktionsanalyse, for at belyse de tilstedeværende diskurser. Dette er valgt, da det er interessant at se på de meninger og holdninger participanterne ytrer, både verbalt samt gennem deres fysiske handlinger under testsituationen. På den måde, fås et dybere indblik i deres forståelse for, og holdninger til, kursets indhold.

Der zoomes ud i rapporten ved at have fokus på de større teorier inden for organisationsteori, herunder Jaffee og Burris, hvortil vi hæfter den indsamlede empiri. Herved startes der med at se på lokale praksisser fra et bredt perspektiv, hvorigennem der ses på sikkerhedskurserne i en større sammenhæng.

Repræsentering af praksisser ved at zoome ind på hvad der bliver sagt og gjort

Det første Nicolini vurderer som et vigtigt fokuspunkt i undersøgelsen af praksisser, er selve det der bliver sagt og gjort.

„What distinguishes a practice-based approach is that what in traditional accounts appears as a given is seen and described here as a skilled accomplishment “ (Nicolini, 2009, s. 1400)

Et eksempel herpå kunne være en sygeplejerskes telefonsamtale med sin patient. Det beskriver Nicolini som værende måden hvorpå samtalen holdes i et godt tempo, det specifikke ordvalg og styringen af selve samtalen. Disse er allesammen elementer, der essentielt set er et resultat af sygeplejerskens færdigheder (Nicolini, 2009).

Det er relevant at se situationelle praksisser som et sæt af organiserede sproglige, såvel som fysiske handlinger. Nicolini beskriver at ved at zoome ind på praksis ud fra et etnografisk synspunkt, kan praksisser på den måde undersøges gennem medierede redskaber.

Nicolini forklarer ydermere, at for at forstå praksisser i helhed, kræver det at fokusset rettes mod at forstå alle elementers rolle som går ind i opbyggelsen af en praksis. „The saying is a way of doing as much as the doing is in what is said or not said“ (Nicolini, 2009, s. 1400). Med dette citat forklarer Nicolini, at praksisser både har en materiel såvel som en diskursiv dimension. Det er derfor ikke kun den sproglige rolle, som har betydning for forståelsen af kommunikation i praksis. Det er også vigtigt at have fokus på det fysiske kropssprog, for at se hvorvidt det hænger sammen med den diskurs sproget antager. Herunder er det også interessant at se på hvordan det fysiske kropssprog interagerer med den materielle dimension, og se på hvordan personer i praksis agerer med det fysiske miljø. Et eksempel på dette kunne være måden hvorpå sygeplejersken interagerer med dokumenterne omhandlende patientens medicin, samtidig med at hun holder en samtale kørende med patienten.

I undersøgelsen af praksisser, kan der endvidere zoomes endnu mere ind på de kommunikative handlinger i praksis, ved at analysere diskursen af disse. Nicolini forklarer endvidere gennem eksempler med telemedicin, at gennem analyse af diskurser i en samtale kan der fås en mere detaljeret forståelse for, hvordan handlinger skabes gennem kommunikationen. Det giver en bedre forståelse for hvordan virkemidler og andre redskaber inden for diskursteorien, har betydning for opbygningen af kommunikative handlinger i praksis.

zoom ud ved at studere effekten

For at øge forståelsen for praksis, kan der ved at zoome ud igen, fås et indtryk af praksisser i helhed. En måde dette kan gøres på, er ved at se på de lokale og translokale effekter en given praksis har på sit miljø og omgivelser. Nicolini forklarer denne forståelse med eksempler fra sine egne studier af telemedicin *„For instance, the practice under consideration engenders a specific way of being for both the interactants“* (Nicolini, 2009, s. 1409). Her fortæller han at selve praksissen af telemedicin i helhed, har givet anledning til at begge aktører i denne sammenhæng har påtaget sig bestemte roller. Den har derfor påvirket og forandret de klassiske læge-patient roller, til en velinformeret patient, som fra start kan indgå i en dialog baseret på lægefaglige begreber. Derudover har denne direkte kontakt mellem sygeplejersken og patienten også påvirket den klassiske kontaktform, og på den måde skabt et tæt bånd mellem disse, som differentierer sig fra den måde tingene plejer at blive gjort.

Situationel kommunikation kan altså have en overordnet indflydelse på elementerne omkring denne. Aktørernes deltagelse har potentiale til at påvirke deres væremåde, og eventuelt deres opførsel efterfølgende.

Nicolini forklarer yderligere, at for at forstå og analysere praksissers relation til deres effekter, kan der benyttes det teoretiske og metodiske værktøjssæt inden for sociologien. *„in order to study empirically the connected-ness of practice through its effects, we can employ the theoretical and methodological toolkit of the sociology of translation.“ (Nicolini, 2009, s. 1410)*. Teorien beskriver nogle centrale begreber fra det tidligere nævnte værktøjssæt som hjælper med at opretholde forbindelsen mellem praksisser. Disse begreber vil blive beskrevet nedenunder.

Mediators

Mediators er elementer som understøtter forbindelsen mellem praksisser. Disse inkluderer grænseobjekter, såsom navne, planer og regler, og fungerer som Generalizers og Localizers.

Generalizers

Mediators som generalizers, opsummerer og formidler viden og erfaring fra adskillige praksisser, og gør det til genstand for videre arbejde i andre praktiske kontekster. Nedenstående er et eksempel givet af Nicolini. *„Human experts 'summarize' years of learning by doing, and artefacts such as the portable ECG black box, the work and knowledgeability of all those who designed and built it“ (Nicolini, 2009, s. 1411)*. Det er igennem et medieret arbejde med disse, at lokale praksisser skaber, hvad Nicolini beskriver som *macro phenomena* (Nicolini, 2009). Macro phenomena er en kompleks samling af handlinger og verbale ytringer, steder og objekter som kan observeres på tæt hold (Nicolini, 2009).

Localizers

Mediators som localizers, er når mediators fungerer som en slags indgang, hvor større og mere stabile praksisser kan etablerer deres tilstedeværelse i den lokale praksis. Nicolini eksemplificere sygeplejerskens brug af protokollen „The protocol translates, in this local instance, the previous work, power and legitimacy of the vast practice-net of 'scientific medicine“ (Nicolini, 2009, s. 1411).

Localizers er derfor indgangen hvorigennem erfaring fra tidligere praksisser, og det arbejde der er lagt i disse, kan udmunde sig i form af et værktøj i den lokale praksis, til fordel for aktørerne.

At zoome ud fra den lokale praksis er et godt værktøj til at give et overblik over, hvilken effekt denne har på sine omgivelser. Dette giver derudover mulighed for at følge effekten gennem de givne mediators, og på den måde få en ide om hvor meget denne breder sig ud over den lokale praksis.

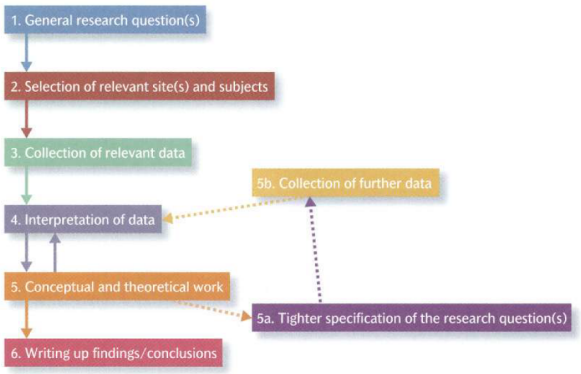
Metode 5

I dette kapitel vil der blive redegjort for de anvendte empiriindsamlingsmetoder. Der vil være en generel introduktion til hvad kvalitative metoder er, en gennemgang af interviewteori, herunder brugen af interviewguides samt fokusgruppeinterview, og dertilhørende videoobservation. Ydermere vil der være en gennemgang for brugen af interaktionsanalysen samt hvilket formål denne har.

5.1 Kvalitativ metode

Dette afsnit vil fokusere på kvalitative metoder som er essentielle for vores projekt, da de sikrer en meget holdningsbaseret mængde data som kan bidrage til at undersøge problemstillingen.

Kvalitativ forskning er blevet en stadig mere populær tilgang til social forskning. Kvalitativ forskning er en forskningsstrategi, der hovedsageligt fokusere på ord fremfor kvantificerbar data i indsamling og analyse af data. Der findes mange måder at indsamle kvalitativ data, herunder interview, observation og fokusgrupper, som har til formål at undersøge deltagernes subjektive holdninger. Der vil i projektet blive anvendt både interview, obervationsstudier og fokusgruppeinterview. De tre metoder er udvalgt da de passer godt til projektets tilgang og kan hjælpe med at tilkendegive subjektive holdninger til IT-sikkerheden hos COWI.



Figur 5.1. Kvalitativ metode process (efter (Bryman, 2014, s. 384)

Den ovenstående figur er udviklet af Alan Bryman, og indeholder seks overordnede faser der hjælper til at repræsentere processen ved brug af kvalitative metoder. Den første fase er hvor der udarbejdes generelle forskningsspørgsmål, og hvor eventuelle tidligere lignende forskning undersøges. I anden fase vælges der relevante perspektiver og emner, som ligger til grund for forskningens vinkel. Det er også i denne fase den korrekte målgruppe for undersøgelsen findes. En repræsentativ målgruppe er meget vigtigt for validiteten af dataen. I den tredje fase indsamles

den relevante data. I denne fase skal indsamlingsmetoden vælges, hvilket bør overvejes grundigt, da det har stor betydning for hvilken data der kan opnås. I den fjerde fase bliver den indsamlede data analyseret. Denne fase vil være forskellig ud fra hvilken kvalitativ metode der anvendes. Her vil der kunne opstå ny viden efter dataene er blevet analyseret. Denne nye viden kan be- eller afkræfte tidligere antagelser, hvilket kan skabe en ny vinkel. Den femte fase er hvor den indsamlede data analyseres teoretisk, hvilket muliggør perspektivering. Fra denne fase kan forskningsspørgsmålet specificeres, for dernæst at indsamle data på ny, men det er også muligt at gå direkte tilbage til den forrige fase. Dette gøres da nye vinkler kan opstå, som kræver nærmere undersøgelse. I den sjette fase opsamles der på den kvalitative undersøgelse, og det teoretiske arbejde evalueres. I denne fase skulle forskningsspørgsmålet gerne kunne besvares (Bryman, 2014).

5.1.1 Betragtninger ved brug af Kvalitative metoder

Der er mange betragtninger der bør overvejes inden brug af kvalitative metoder. Alan Bryman nævner fem ting der bør overvejes før kvalitativ forskning startes. En af dem er at sætte sig ind i participanternes perspektiv. Det er vigtigt at forskere er i stand til at sætte sig i deres participanternes sted, for at kunne forstå holdninger, og sætte dem i relation til personens omgivelser. Der kan derfor være mange forskellige svar, hvilket kan være med til at gøre kvalitative metoder besværlige. En anden betragtning der bør overvejes er subjektive holdninger. Hvis en forsker har en subjektiv holdning til emnet, er det meget vigtigt at dette ikke påvirker analysen af den indsamlede data, da dette manipulere det egentlige resultat. Forskeren skal forsøge at se det fra participanternes perspektiv, for at opnå et mere objektivt resultat. Det bør også overvejes, at det kan være svært at genskabe dataindsamlings-situationer, da indsamlingen ofte er meget ustruktureret, samt at den er afhængig af hvordan hele processen er forløbet. Ved brug af eksempelvis ustruktureret interview, vil participantens svar være med til at forme interviewet, og derfor være unikt. En anden betragtning er at den data der opnås er meget subjektiv. Det er derfor vanskeligt at generalisere ud fra den fundne data, og konkludere noget om en større gruppe mennesker. I stedet for at fortælle noget om store grupper, kan der udledes mere specifikke holdninger, som kan være med til at be- eller afkræfte antagelser. En sidste betragtning der bør overvejes ifølge Bryman er gennemsigtighed. Det kan være vanskeligt at gennemskue en forskers fremgangsmåde ved brug af kvalitativ metode. Grundet at processen og resultatet er så forbundet, er det vigtigt at beskrive processen for at gøre sine resultater mere gennemskuelige og pålidelige (Bryman, 2014).

5.2 Interview

I dette afsnit vil teorien bag interviewet blive forklaret. Der vil være en redegørelse for den valgte interviewstruktur, samt interviewguidens formål. Ydermere vil retningslinjerne for en transskription blive forklaret. Foruden ovenstående vil der forekomme en forklaring af fokusgruppeinterviews, herunder brugen af videoobservation. Interviewmetoden er valgt for at få en dybere forståelse for medarbejdernes holdninger til IT-kurserne samt hvilke udfordringer de føler er opstået ved brugen af disse kurser.

5.2.1 Det semistrukturerede interview

Der er tre former for interviewstruktur: det åbne interview, det semistrukturerede interview og det strukturerede interview. Til denne rapport er det semistrukturerede interview blevet valgt, da det giver frihed og mulighed til at følge meninger, der kommer til udtryk under interviewet. Det bevarer ydermere en åbenhed til det undersøgte emne, men stadig med en form for struktur gennem den udarbejdede interviewguide, som sikrer at de stillede spørgsmål er relevante. Fleksibiliteten af det semistrukturerede interview gør det muligt at udforske områder, der kommer frem under interviewet, som kunne have relevans for problemformuleringen. Interviewet muliggør en sammenkobling af det teoretiske udgangspunkt med ny empiri og på baggrund af dette vælges det semistrukturerede interview (Kvale & Svend Brinkmann, 2015).

5.2.2 Interviewguide

Som nævnt tidligere giver en interviewguide interviewet en vis form for struktur. Den kan ses som et manuskript for interviewet og variere i struktur alt afhængig af den valgte interviewform. I dette projekt er fokusgruppeinterviewet en af de valgte metoder, hvor en direkte tilgang er valgt. Før interviewet informeres interviewpersonerne om at der er fokus på IT-kurserne og forståelsen af disse. Strukturen kommer i form af en række spørgsmål. Disse spørgsmål vurderes ud fra to dimensioner: dynamik og tematisering. Fokusset i den dynamiske dimension ligger i spørgsmålene *hvordan* og har til formål at *„fremme et positivt samspil, holde samtalen i gang og stimulere interviewpersonerne til at tale om deres oplevelser og følelser“* (Kvale & Svend Brinkmann, 2015, s. 186). Den tematiske dimension relateres til forskerens teoretiske opfattelser af undersøgelsens emne og dertil analysen af interviewet. Spørgsmålene der stilles her er *hvad* og varieres på bagrund af forskerens hensigt med interviewet. Under foksugruppeinterviewet belyses meninger og holdninger til et givent emne: *„livlige, kollektive ordveksling kan bringe flere spontane ekspressive og emotionelle synspunkter frem“* (Kvale & Svend Brinkmann, 2015, s. 206). De to dimensioner kan komme til udtryk i et spørgsmål, men *„Et begrebsmæssigt godt, tematisk forskningsspørgsmål er ikke nødvendigvis et godt dynamisk interviewspørgsmål“* (Kvale & Svend Brinkmann, 2015, s. 186). Spørgsmålene i interviewguiden har derfor to formål; *„tematisk bidrage til produktionen af viden og dynamisk fremme et godt interviewsamspil“* (Kvale & Svend Brinkmann, 2015, s. 185). Forståelsen for begreber kan variere, hvilket kan skabe misforståelser og eventuelle manglende svar. Dette er en vigtig pointe at have med når interviewguiden laves.

5.2.3 Fokusgruppeinterview

Fokusgruppeinterviews er en metode for forskeren til at forstå, hvorfor folk føler som de gør om et givent emne. Det har den fordel at det, som interview, vil give et mere realistisk billede, da interaktionen mellem gruppens medlemmer stimulerer ægte og nuancerede udsagn. De informationer, som fremkommer gennem denne interaktion, vil have en større styrke og klarhed end ved brugen af et traditionelt interview. Ydermere virker interaktionen også som en form for kontrol på ekstreme eller falske oplysninger, da deltagerne har muligheden for at give hinanden mod- og medspil. Dette skaber en dynamisk dialog, og vil oftest medføre at udsagnene er relevante og væsentlige, som muligvis ikke ville være kommet til lys under et traditionelt interview.
Et fokusgruppeinterview har et snævert syn vedrørende emnet, hvilket står i kontrast til

gruppeinterviewet. Forskeren skal begrænse sig til færre emner grundet antallet af deltagere. Dette virker som en svaghed for fokusgruppeinterviewet, men ikke under dette projekt, da fokusset for projektet er indsnævret til ét aspekt af den undersøgte organisation. Forud for interviewets start blev alle participanterne bedt om at underskrive en samtykkeerklæring (J.f H).

Videoobservation

Videoobservation er en afgrening af observationsmetoden og muliggør en gengivelse af fænomener i sin eksakte, multimodale form. Dette vil sige, at modsat lydoptagelse, kan videoobservation fastholde kropsliggjorte og kontekstafhængige handlinger. Hermed menes det, at forskeren ikke kun er interesseret i hvad participanterne siger, men også brugen af deres kropssprog samt hvordan de agere i konteksten. De filmede fænomener eller objekter, er teoretisk betingede valg (Alrø & Lone Dirckinck Holmfeld, 2001). Ikke nok med at videoobservation gengiver et udsnit af virkeligheden og samtidig formidler budskabet på en forståelig måde, så kan denne form for observation gøre forskeren opmærksom på forhold, der har en indvirkning på interaktionen mellem participanterne, som kan være utydelige. Empirien, samlet i dette projekt, er etnometodologiske, da de handlinger der undersøges forsøger at opnå et givent institutionelt mål (J.f 2.4).

5.2.4 Transskription

Ud af Steinar Kvales syv interviewfaser er transskriptionen den fjerde, og omhandler måden hvor forskeren går fra samtale til skreven tekst. Denne tekst kan komme i form af udskrifter, hvilket vil være tilgængelig for videre analyse (Kvale & Svend Brinkmann, 2015).

I forlængelse af interviewet, besluttede vi os i projektgruppen for at videooptage interviewet. Grundlaget for dette var at sikre dokumentationen af interviewet som efterfølgende kunne bruges til udarbejdelsen af analysen (Kvale & Svend Brinkmann, 2015). Videooptagelser giver moderatoren frihed til at fokusere på participanterne og deres udtalelser, så de relevante udsagn fra participanternes side kan uddybes løbende. Foruden dette, giver videooptagelsen mulighed for at se interviewet flere gange, hvilket mindsker risikoen for at relevant data overses. Som nævnt tidligere, er transskribering at gå fra mundlig tale til en skreven form. Dette kan ses som den første fase i den analytiske proces (Kvale & Svend Brinkmann, 2015). For at sikre en kontekstuel forståelse, blev det besluttet, at en af de tilstedeværende interviewere skulle transskribere interviewene. Udsagnene skulle skrives ned uden at tolke på dem, men fyldeord såsom "øh", "øhm"osv. blev dog ikke skrevet ned. Dette skulle være behjælpelig til en bedre analyseproces. I transskriptionerne vil der enkelte steder forekomme tidsstempler. Disse indikerer passager hvor participanterne snakkede i munden på hinanden hvilket, gjorde det umuligt at høre hvad der blev sagt.

5.3 Diskursanalyse

I led med rapporten vil vi have fokus på diskursanalyse, hvor vi først vil definere hvad diskursanalyse er på en overordnet plan, for senere at benytte det i interaktionsanalysen.

Inden for diskursbegrebet findes der mange forskellige definitioner. En definition der dækker begrebet bredt, lyder på „a specific ensamble of ideas, concepts, and categorisations that are

produced, reproduced and transformed in a particular set of practices“ (Hajer, 1995, s. 44). Ved denne definition af diskursbegrebet ligger der en forståelse af, at den sociale betydningsdannelse er organiseret i nogle sæt af udsagn, begreber og kategoriseringer. Derfor er der ved denne tradition for diskursanalyse ikke direkte fokus på den konkrete tale eller sociale handling, men dens såkaldte mulighedsbetingelser, som konstituerer konkret menings- og vidensdannelse. Det konstituerende element ligger i, at fænomener italesættes, ikke blot i den forstand at vi taler om dem, men også i den forstand at fænomenerne bliver begribelig for os i kraft af diskursen (Horsbøl & Pirkko Raudaskoski, 2016).

Der vil i projektet anvendes en interaktionsanalyse til at udføre diskursanalysen. Interaktionsanalysen har til formål at undersøge diskurs, da der igennem den konkrete betydningsdannelsen, som finder sted her og nu, kan fremhæves medarbejdernes holdninger og meninger til IT-kurset. Dette gøres bedst igennem en interaktionsanalyse, da der ved observation af vores participanters udførelse af IT-kurset, kan dannes en forståelse for hvordan de opfatter, italesætter og interagere med COWIs IT-sikkerhedskursus.

5.4 Interaktionsanalyse

Vi vil som nævnt i afsnit under rapporten foretage en videoobservation (J.f 5.2.3) af COWI medarbejdernes udførelse af et givent IT-kursus omhandlende e-mail sikkerhed, med henblik på at analysere det kommunikative aspekt samt interaktionerne mellem disse. Vi har her interesse i, gennem en kommunikationsanalyse, at undersøge hvordan sikkerhedsinstrukser og kursets indhold bliver formidlet og forstået, til og imellem medarbejderne. Test situationen har igennem „situated action perspective“ til formål at belyse eventuelle udfordringer i overførelsen af kommunikative handlinger, for at forhindre en øget sikkerhedsrisiko for virksomheden COWI.

5.4.1 Metodisk fremgang

I projektet anvendes der interaktionsanalyse indenfor diskurs. Denne diskursanalyse er valgt, da projektet vil undersøge meningerne og medarbejdernes forståelse for kursets indhold, ud fra deres fysiske handlinger samt verbale ytringer som bliver udtryk undervejs. Dette vil blive forklaret yderligere i de følgende afsnit. Som Nicolini fortæller.

„What distinguishes a practice-based approach is that what in traditional accounts appears as a given is seen and described here as a skilled accomplishment“ (Nicolini, 2009, s. 1400)

Som det ses af citatet, kan den indsamlede empiri uddybes, ved at analysere og fokusere på selve konstruktionen af medarbejdernes handlinger i praksis, og hvad disse betyder for deres forståelse. Interaktionsanalysen gør netop dette. Ved at undersøge medarbejdernes handlinger i praksis, både igennem det fysiske kropssprog og verbale vendinger, kan der på på den måde opnås en indsigt i hvor godt og hvordan kursets indhold forstås.

Ved analyse af den indsamlede empiri, søges der derfor at få en forståelse for praksissen i helhed, herunder medarbejdernes forståelse, og de elementer der går ind i konstruktionen af medarbejdernes handlinger.

Praksisser har som tidligere nævnt af Nicolini, både en materiel og en diskursiv dimension. Derfor, som Nicolini argumentere, er det ikke nok bare at have fokus på det diskursive aspekt af praksissen. Som der ses af citatet nedenunder.

„the saying is a way of doing as much as the doing is in what is said or not said“ (Nicolini, 2009, s. 1400)

Det er ligeså aktuelt at undersøge den fysiske dimension hvorved situation tager sted. Med det menes der, at i sammenhæng med analysen af sprogets diskurs, er det vigtigt at kigge på medarbejdernes kropssprog, for at se hvorvidt meningerne og forståelserne der udtrykkes her, følger den sproglige diskurs. Derudover ses der også i den materielle dimension på hvordan det fysiske miljø bruges af medarbejderne under kursets forløb, da måden de interagerer med de tilstedeværende redskaber, også er en indikation af deres forståelse for kursets indhold.

Interaktionsanalysen implementere netop det Nicolini foreslår, ved at zoome ind på hvad medarbejderne siger og gør i praksis via interaktionsanalysen, og derved undersøge hvordan deres holdninger kommer til udtryk gennem verbal kommunikation og kropslige udtryk.

5.4.2 Situated action perspective i den lokale praksis

Ilpo Koskinen beskriver i sin rapport „Utilizing Situated Action Perspective in Usability Testing“ begrebet „situated actions“ som er erhvervet fra Lucy Suchmans bog ved samme navn, og oversættes til „lokaliserede handlinger“.

Lokaliserede handlinger omhandler brugernes handlinger og den situationelle påvirkning under den lokale praksis, hvilket i denne kontekst er testsituationen. Her er der fokus på hvordan brugerne sammenfatter deres handlinger og beslutningstagningen ift. de midler de har til rådighed i en given situation. Det interessante for os ved „the situated action perspective“, er her at se på hvordan medarbejderne formidler sikkerhedsinstrukser fra organisationen til handlinger, og hvordan de situationelle elementer påvirker denne proces (Koskinen, 2000a).

Miljøet spiller en stor rolle for at få en realistisk repræsentation af brugerens handlinger, og derfor forsøges der at holde omgivelserne så naturlige som muligt, for her at undgå eventuelle forstyrrelser. Testen foretages derfor på medarbejdernes arbejdsplads, COWI Aalborg, iblandt kollegaer der kender hinanden på forhånd.

Hertil blev interaktionsanalysen som led i Nicolini's "zooming in" fase brugt til at få et dybere indblik i medarbejdernes *situated actions* i den lokale praksis.

5.4.3 Interaktionsanalysens teoretisk grundlag

Ved interaktionsanalysen tages der afsæt i sociologen Garfinkels udvikling af filosofferne Husserls og Schutzs fænomenologi. Hvor der førhen udelukkende har været fokus på at betragte fortolkning som et fænomen der foregår inde i selve individet, vægter Garfinkel i stedet at opfatte fortolkning som et offentligt tilgængeligt fænomen der foregår i den igangværende handling. Dette kaldes for etnometodologi. Etnometodologi anser samfundsmæssige og kulturelle fænomener som en kontinuerlig dannelse i almindelige menneskers adfærd. Dermed er etnometodologiens fokus på praktiske hverdagshandlinger og især på den lokale, intersubjektive opnåelse af betydning og meningsdannelse. Inden for etnometodologien er der en vis interesse i 'etnometoder'. Etnometoder kigger på hvordan mennesker i forskellige miljøer sammen formår at udføre en given situation, og hvordan de gennem handlingerne og rækkefølgen af disse handlinger italesætter hvorledes de forstår den given situation. Dette kommer til udtryk i form af handlinger som lingvistiske og kropslige fænomener, der udspiller sig i det materielle

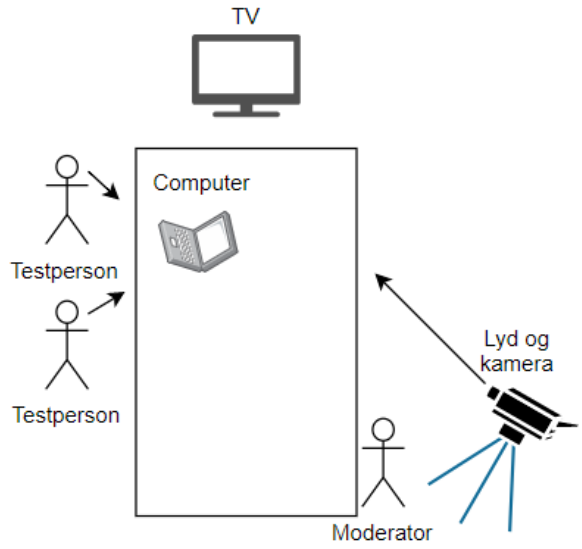
miljø. Diskurs forstås derfor i denne sammenhæng som konstitueret gennem (multimodal) betydningsdannelse (diskurs) i praksis (handlinger). Ved den multimodale interaktionsanalyse er der ikke kun rettet fokus på hvad der bliver sagt. Gennem analyse og observering af, hvordan respondenterne gør brug af kropssprog og materielle omgivelser for at fremme og konstituere betydningsdannelsen blandt parterne, opnås der en bedre konsensus af, hvordan disse semiotiske handlinger samt materialitet er tæt knyttet til selve betydningsdannelsen i situationen. Det skyldes at når vi mennesker deltager i forskellige interaktionssituationer, benytter vi en række multimodale elementer såsom sproget, kroppen, gestik, ansigtsudtryk, artefakter og stedet, for at fremme betydningsdannelsen overfor de øvrige parter. Derfor betragtes diskurs inden for interaktionsanalysen ikke kun udelukkende som tekst eller tale, men som brug af de eksisterende materiel-semiotiske ressourcer i den gensidige konstitution af social orden (Raudaskoski & Malene Kjær, 2016).

5.4.4 Interaktionsanalyse testopsætning

Vi har i led med rapporten foretaget en interaktionsanalyse af otte medarbejdere hos COWI. Dette gøres med henblik på at analysere hvordan vores participanter opfatter, forstår, italesætter og interagere med hinanden og COWIs IT-sikkerhedskurser, som de bliver eksponeret for tre gange årligt. Interaktionsanalysen fokus retter sig mod at undersøge hvordan sikkerhedsinstrukserne bliver formidlet og forstået, til og mellem medarbejderne. Valget om at udføre IT-kurserne med to participanter ad gangen, havde til formål at simulere thinking aloud som metode, hvor en partipant skal verbalisere alle sine tanker og holdninger, imens de bevæger sig igennem en angiven brugergrænseflade. Thinking aloud som metode blev dog fravalgt, men dog stadig draget en del inspiration fra. Fravalget af thinking aloud er grundet, at to participanter der har en åben dialog, vil danne en mere naturlig ramme for vores participanter, kontra at sidde alene og verbalisere sine tanker og holdninger til kurset. Det er med til at skabe en mere naturlig og reel dialog mellem vores participanter, der åbner op for eventuelle emner der ellers ikke ville have været berørt. Vi instruerede i stedet vores participanter i at have en åben dialog kørende, hvori de skulle dele deres tanker, overvejelser og begrundelser for deres svar mellem hinanden imens de udførte IT-kurset. Dette havde til formål at give en mere dybdegående refleksion af IT-kurset blandt vores participanter og deres holdninger hertil. Det skyldes at participanters holdninger og meninger bedre vil komme til udtryk gennem verbal kommunikation og kropslige udtryk ved en åben dialog sammen med en af deres kollegaer, end hvad en enkelt participant der udførte kurset alene ville have givet os af empiri. Som tidligere nævnt dannede dette en mere naturlig ramme for vores participanter, og var derfor noget participanterne lettere kunne forholde sig til.

Vi har forud for interaktionsanalysens påbegyndelse besøgt COWI, og gennemgået de tre årlige kursusmaterialer medarbejderne skal igennem. Det har vi gjort med formålet om, at få en så bred forståelse som muligt for de informationer samt øvelser vores participanter bliver eksponeret for gennem sikkerhedskurset. Ligeledes har vi besøgt og undersøgt de lokaler testen skulle foregå i forud for testens start, for at finde den optimale placering af kamera, der kunne give den bedste videoobservation af vores participanters interaktioner mellem hinanden samt kursets indhold. Kurset blev udført i to forskellige lokaler, dog med den præcis samme testopsætning. Miljøet spiller en stor rolle for at få en realistisk repræsentation af brugerens handlinger, og derfor forsøges der at holde omgivelserne så naturligt som muligt for participanterne, her for at undgå eventuelle forstyrrelser. Derfor blev testene udført ude ved COWI, såvel som der blev valgt kun

at have en af gruppens medlemmer til stede under selve testen. Computeren der blev brugt i led med udførelsen af IT-kurset, blev koblet til TV'et via. et HDMI-kabel. Det muliggjorde at kameraets placering både kunne optage vores participanters interaktioner og reaktioner mellem hinanden såvel som på kurset. Testens opsætning ses på figur 5.2.



Figur 5.2. Testopsætning

5.5 Indholdsanalyse

Når der skal analyseres kvalitativ data fra interviews, findes der adskillige metoder at gøre brug af, og flere forskellige aspekter at have fokus på. De mulige analytiske værktøjer hører hovedsageligt til under to kategorier, fokus på mening eller fokus på sprog. Vi har valgt at have fokus på meningen i analysen af fokusgruppeinterviewene, da vi er interesserede i at se på holdningerne der blev udtrykt under fokusgruppe interviewene.

Til at forstå og få yderligere indblik i medarbejdernes perspektiv og holdninger, har vi valgt at benytte os af en indholdsanalyse til at analysere fokusgruppeinterviewene. Denne analyseform hjælper os med at kondensere interviewet, og uddrage de centrale temaer i interviewene, som vil give os et mere detaljeret indblik i medarbejdernes holdninger til IT-sikkerhed.

Vi har taget udgangspunkt i kvale og brinkmanns interviewanalyse med fokus på mening, som vil blive beskrevet yderligere i næste afsnit.

Meningskodning

Meningskodning er et analyseredskab, som hjælper med at reducere og konkretisere lange udtalelser fra interviewpersoner, ved at tildele disse passende nøgleord, og herefter inddele dem i kategorier.

Meningskodning består i at tilskrive et eller flere nøgleord til et afsnit i transskriptionen, som beskriver det udsagn interviewpersonen kommer med. Dette har til formål at hjælpe analytikeren med hurtigt at kunne identificere og finde afsnittet senere hen, og på samme tid give et indtryk af de centrale temaer der kommer til udtryk igennem interviewet (Kvale & Svend Brinkmann, 2009).

Udover kodning kan afsnittene systematiseres yderligere ved at kategorisere afsnittene ud fra de tildelte nøgleord. Herved er der mulighed for at kvantificere hvor tit visse emner bliver nævnt i interviewet, og disse kan herefter sammenlignes med andre målinger. Dette giver analytikeren mulighed for at få et mere systematisk overblik over de gennembrydende temaer i udsagnene (Kvale & Svend Brinkmann, 2009).

Meningskondensering

Til at analysere den indsamlede empiri fra fokusgruppeinterviewene, bruges meningskondensering til at reducere meningsindholdet, og skabe overblik over de centrale temaer som kommer frem igennem interviewpersonernes udsagn. Processen består i at gennemlæse interview transskriptionen, identificering af meningsenheder og kondensering af det centrale tema.

Det første skridt i analysen, er at læse transskriptionen af interviewet igennem. Ved at læse denne igennem en eller flere gange, har analytikeren mulighed for at fordybe sig i teksten, og få et mere detaljeret overblik over udsagnene i interviewet.

Under gennemlæsningen af transskriptionerne identificeres de naturlige meningsenheder, som fremkommer af interviewpersonernes udsagn.

Herefter omformuleres meningsenhedernes gennemgående tema ned til en central beskrivelse på få linjer, bestående af dennes hovedbetydning.

Meningsfortolkning

For at få en dybere forståelse for interviewudsagnenes temaer, vil vi benytte os af meningsfortolkning.

I modsætning til meningskondensering, rækker meningsfortolkning ud over selve det der bliver sagt og gjort under interviewet. Her er fokus på at forstå og udforske udsagnene ved at tolke på dem ud fra analytikerens synspunkt.

„Fortolkningen af meningsindholdet i interviewtekster rækker ud over en strukturering af det manifeste meningsindhold i det, der siges, og omfatter dybere og mere kritiske fortolkninger af teksten“ (Kvale & Svend Brinkmann, 2009, s. 230).

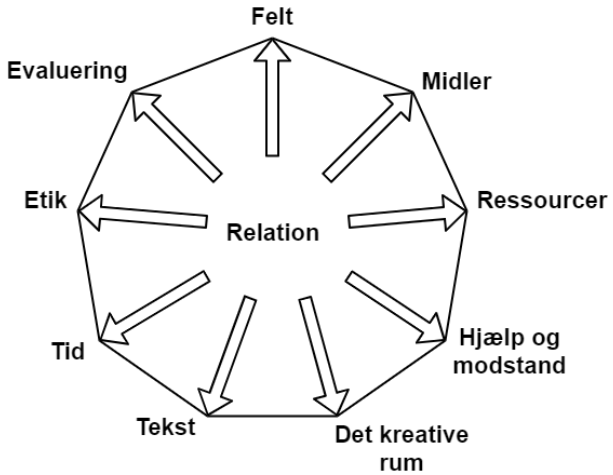
Ved at fortolke det meningsindhold, som bliver identificeret i transskriptionen, kan der findes betydningsrelationer og meningsstrukturer der ikke ikke er præsenteret i selve udsagnene (Kvale & Svend Brinkmann, 2009). På den måde kan der som analytiker findes frem til en dybere og mere detaljeret beskrivelse af meningerne, som bliver ytret af interviewpersonerne.

Analyse 6

I vores analysearbejde vil vi analysere den interne strategiske kommunikation, baseret på Hallahans definition derpå (Hallahan et al., 2015, s. 3). Analysen vil lægge vægt på at opbygge en forståelse for medarbejdernes holdninger til COWIs IT-sikkerhedskurser, og udfordringer der opstår derved. Rapportens fokus vil ligge i organisationens intraorganisationelle niveau (J.f 4.1). For at forstå COWIs kommunikationsituation vedrørende deres anvendte IT-kurser vil vi benytte diamantmodellen (J.f 6.0.1). Heraf vil vi analysere IT-kurset i en brugskontekst ved brug af en interaktionsanalyse (J.f 6.1), som foretages ud fra observationstudier af IT-kurserne. Denne analyse vil være baseret på Nicolinis tanker om situerede handlinger (J.f 4.3), og vil i praksis undersøges i fire grupper af to personer, for at få en åben dialog, hvor vi kan undersøge medarbejderens interaktion mellem hinanden og med kurset. Herefter vil en indholdsanalyse (J.f 5.5), baseret på det udarbejdede fokusgruppeinterview fortages, hvor de førnævnte to-personers grupper, samles i to grupper af fire. Heri kan vi få et mere generelt indblik i praksis og identificere udfordringer i led med anvendelse af IT-kurser i COWI.

6.0.1 COWI ud fra Diamantmodellen

Diamantmodellen er lavet med henblik på planlægning af kommunikation i og fra organisationer. Den indeholder 10 facetter, som samlet giver et bredt perspektiv på kommunikationen (Hestbæk Andersen & Flemming Smedegaard, 2012). Vi benytter modellen til at få en forståelse for COWIs kommunikationssituation når det kommer til IT-sikkerhed, hvor fokusset i denne kontekst lægger på deres IT-sikkerhedskurser. Interviewet med COWIs CIO, samt empiri fra casebeskrivelsen, ligger til grund for den analyserede data i diamantmodellen. Diamantmodellen ses visualiseret i nedenstående figur 6.1.



Figur 6.1. Diamantmodellen efter (Hestbæk Andersen & Flemming Smedegaard, 2012, s. 22)

Relation:

Relation omhandler forskellige typer af deltagere som agerer i kommunikationen og deres indbyrdes hensigter, mål og relationer. Denne facet kan som den eneste ikke undværes, da deltagere er nødvendige for at kunne opnå kommunikation (Hestbæk Andersen & Flemming Smedegaard, 2012). De deltagende i kommunikationen er alle medarbejdere, der deltager i et IT-sikkerhedskursus. COWI har kun købt licenser til fastansatte, hvilket vil sige at f.eks. konsulenter ikke deltager i kurserne. Ledelsen har til hensigt at udruste de ansatte til at kunne modstå eventuelle hackerangreb. Deres mål er at kunne undgå det helt, men det er ikke muligt, da trusselsbilledet konstant ændres.

Feltet: Feltet handler om emnet, der skal kommunikeres og har en afgørende betydning for om kommunikation kan etableres, idet modtager skal blive opmærksom på og acceptere invitationen før kommunikation kan finde sted (Hestbæk Andersen & Flemming Smedegaard, 2012). Feltet der skal kommunikeres er IT-sikkerhed. Det gøres, i relation til opgavens emne, med IT-sikkerhedskurser, som er udvalgt fra en større samling, alt efter hvad der skal være fokus på i det givne år. Det kan være et problem at nogle ikke finder det interessant, og dermed kan mangle motivation til at sætte sig ind i de givne problemstillinger.

Midlerne: Midler omhandler valg af kommunikationsvej og medier. Før en kommunikationsvej vælges bør der laves overvejelser omkring emnet og modtageren for at sikre en passende kommunikation (Hestbæk Andersen & Flemming Smedegaard, 2012). COWI gør brug af intranettet til at gøre IT-sikkerhedskurserne tilgængelige for deres ansatte. Det gør at det kun er ansatte med en konto til deres interne portal der kan deltage, hvilket potentielt kan være med til at gøre det mere trygt at bruge, da det er udbudt af COWI på deres lukkede portal. Der skabes imidlertid en risiko da nogle deltidsansatte og eksterne konsulenter ikke har adgang til kurserne, og derved måske ikke har fået nødvendig undervisning i IT-sikkerhedsforanstaltninger.

Ressourcer: Ressourcer dækker over de forskellige økonomiske, informationsmæssige og menneskelige faktorer, som kontinuerligt bør overvejes fra planlægningsfasen gennem løsningsfasen og gennemførelsesfasen samt evalueringsfasen til sidst, i en kommunikationsindsats (Hestbæk Andersen & Flemming Smedegaard, 2012). COWI bruger en del økonomiske ressourcer på at modstå fremtidige IT-trusler. De er blandt dem, der bruger flest ressourcer inden for ingeniørfeltet(*COWI opgraderer it-sikkerheden*, 2019), og føler derfor de er godt dækket ind mod IT-trusler.

Hjælp og modstand: Hjælp og modstand omhandler de faktorer, der henholdsvis kan fremme eller hæmme den planlagte kommunikation. Herunder bør samfundsudvikling, tendenser og lovgivning og interesseorganisationer overvejes (Hestbæk Andersen & Flemming Smedegaard, 2012). Medarbejderne får hjælp til at tage kurserne ved at blive mindet om at de mangler at gennemføre dem. Hvis de ikke gennemfører kurserne vil det ende med at deres leder bliver informeret og diskuterer det med den pågældende medarbejder. I takt med at IT-sikkerhed har fået mere fokus i medierne, mener COWIs IT-ansvarlige derfor, at medarbejderne er blevet mere opmærksomme på eventuelle trusler. Da COWIs primære aktivitet er rådgivning, og deres primære indkomst er i konsulenttimer, er der etableret et højt fokus på de menneskelige ressourcer. Den primære arbejdsstyrke har enten en bachelor eller kandidat. De Uddannede er primært inden for ingeniørbranchen, men et stigende antal medarbejdere er fra naturvidenskaben, computer- og IT-uddannelser og fra samfundsvidenskabelige baggrunde.

Kreative rum: Det kreative rum omhandler de kreative ideer, der kan forekomme uafhængigt af systematisk og videnskabelig planlægning. Her handler det om at afprøve nye tiltag og teste grænsen for hvad der er muligt (Hestbæk Andersen & Flemming Smedegaard, 2012). Brugen af IT-sikkerhedskurserne, fremfor eksempelvis at gøre brug af en manual, er med til at gøre det mere spændende og varieret at arbejde med grundet den øgede interaktion.

Tekst: Tekst omhandler selve teksten og valget af de præcise ord, vendinger, billeder, grafiske virkemidler, mm., som skal sikre en god kommunikation (Hestbæk Andersen & Flemming Smedegaard, 2012). COWI har ikke selv udformet IT-sikkerhedskurserne, men købt dem fra det canadiske selskab Terranova Security. COWI har købt 25 forskellige kurser og udvalgt de mest relevante, som så kan skiftes på årlig basis. COWI har forsøgt at gøre det mere personligt ved at tilføje et logo på kurserne. Kurserne er købt i forskellige sprog, så oversættelsen er foretaget af Terranova Security.

Tid: Tid omhandler de tisperspektiver, der kan opstå i planlægningen af kommunikation. Dette dækker over planlægningstid, timing, realiseringstid og krisetid, som der bør være en handlingsplan for (Hestbæk Andersen & Flemming Smedegaard, 2012). Det er vitalt for COWIs fremtidige IT-sikkerhed, at de holder sig opdateret på udviklingen, der sker inden for IT-feltet. IT-sikkerhed er et felt med mange aktører og utrolig hurtig udvikling. Det er også vigtigt at COWI har tilrettelagt en handlingsplan i tilfælde af sikkerhedsbrud, for hurtigst muligt at sikre COWIs aktiver, hvis et angreb skulle finde sted. Det er vigtigt at den er lavet for at kunne stille sikkerhed mod en bred vifte af trusler, og samtidig holde den opdateret over for nye trusler.

Etik:

Etik handler i diamantmodellen om afsenderens virkemidler og de begrænsninger sproget har i forhold til en modtager. Dette skal sikre at modtageren ikke bliver manipuleret med eller vildledt. Kommunikation samt relationen mellem mennesker vil altid stå over for etiske problemstillinger, som bør overvejes grundigt før kommunikation initieres. COWI bør have etiske overvejelser vedrørende dataene, der kommer og sørge for en sikker opbevaring heraf. Dataene skal også sikres i forhold til kursusudvikleren, og sikre sig at de behandler dataene korrekt. Sprogbruget er også en vigtig overvejelse i forhold til de moralske og etiske normer, der er i samfundet. Sproget skal kunne tale til alle og ikke manipulere kursets deltagere.

Evaluering: Evaluering omhandler den fase i processen hvor der er et læringsaspekt. I denne facet kan en pilottest foretages samt en slutevaluering, hvor kommunikationseffekten kan evalueres før og efter den har været i omløb. Før COWI brugte de nuværende IT-sikkerhedskurser udbudt af Terranova Security, benyttede de IT-kurser fra Deloitte. Efter at have evalueret de forhenværende IT-kurser, blev det vurderet at de ikke levede op til forventningerne. Et større problem var at spørgsmålene var så nemme og logiske at der var for lille en udfordring for medarbejderne. COWI evaluerer løbende hvad der er aktuelt for deres ansatte at vide, samt om kurserne er tilstrækkelige.

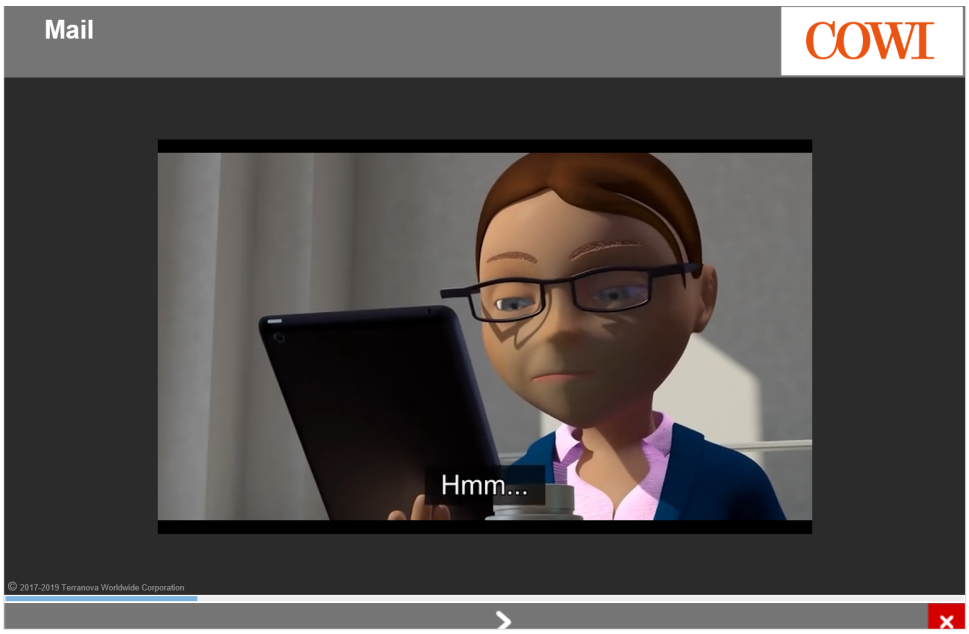
6.1 Interaktionsanalyse

Interaktionsanalysen har til formål at belyse hvordan vores participanter forstår hvad de ser/læser, og undersøge hvordan de igennem deres sprogbrug samt semiotiske handlinger opfatter og forstår disse IT-sikkerhedsmæssige retningslinjer, der bliver udleveret af COWI i

led med IT-kurset. Dette skal give os en forståelse for hvordan participanterne fortolker de oplysninger de bliver eksponeret for i kurset.

Interaktionsanalysen er lavet ud fra fire videoobservationer med medarbejdere fra COWI Aalborg bestående af grupper på to personer, hvor participanter har fået til opgave at gennemgå IT-kurset relateret til e-mails, som de har deltaget i inden for det seneste år. Inden testens begyndelse blev participanterne instrueret i at have en åben dialog om de informationer og øvelser de blev eksponeret for i kurset samt hvad der ellers faldt dem ind i forhold til kurset generelt. Nedestående afsnit er opdelt i sektioner, efter opgavernes kronologiske fremtræden i led med IT-kurset.

Animationsvideo

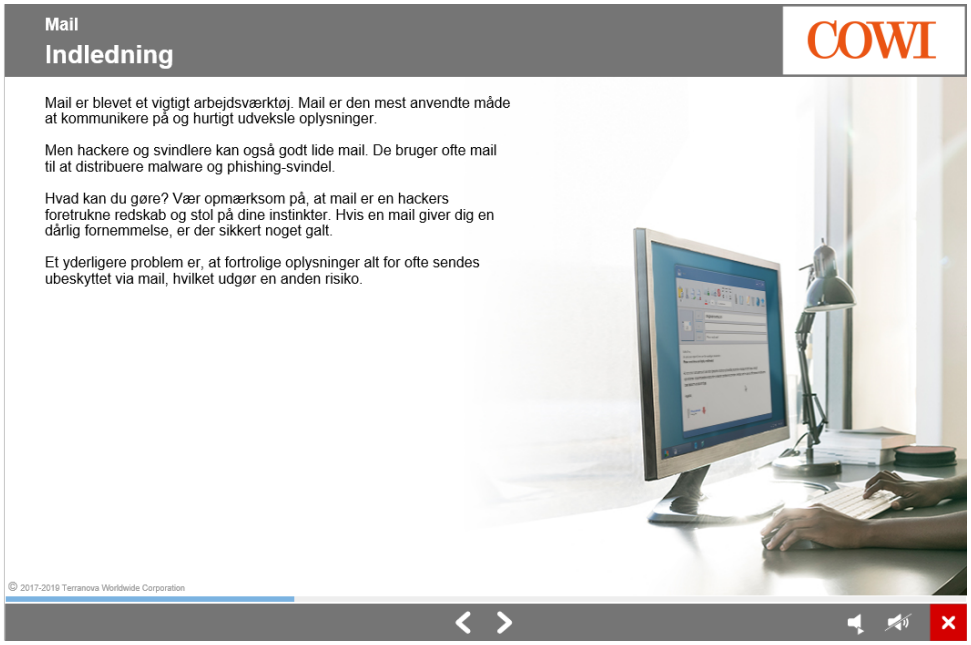


Figur 6.2. Animationsvideo

Alle participanter var umiddelbart positivt stillet over for valget af at anvende animationsvideo, som introducerende måde at formidle information på. Her blev participanterne introduceret for to animationsfigurer, den ene lidt fjollet, som spurgte kluntet om IT-sikkerhedsspørgsmål. Dette resulterede ofte i grin fra participanterne, hvor P3 kommenterede *„Jeg synes det er meget godt, at det sådan er rimelig morsomt“* (J.f B:04), der efterfulgtes af latter, hertil sagde P4 *„Der tænker jeg så, video er rigtig godt til at få ens opmærksomhed“* (J.f B:10). Her anerkendes brugen af humor ikke kun som underholdning, men anses også som værende et godt redskab til at formidle information til de ansatte. Dette er også en holdning, som op til flere af participanterne udtrykte. I forhold til videoen udtalte P6 *„Jeg tror det egentlig er en meget fin måde at gøre det på med den her animationsvideo, for hvis jeg f.eks. tænker på en brochure, tror jeg at man ville lægge den væk, og tænke at den kan man altid kigge på“* (J.f C:03), hvilket indikerer at brug af forskellige interaktionsformer er succesfuld for engageringen af kursusdeltagere. En enkelt participant udtrykte dog også en form for skepticisme overfor animationsvideoen, ved nærmere eftertanke sagde P8 *„Men det tager også lang tid, man skal sidde og vente. Nu sidder vi her og venter også på at den bliver færdig“* (J.f D:42) dette giver udtryk for den høje diversitet

som kurset skal rettes mod, og ikke nødvendigvis altid ender med at være velmodtaget for alle medarbejdere.

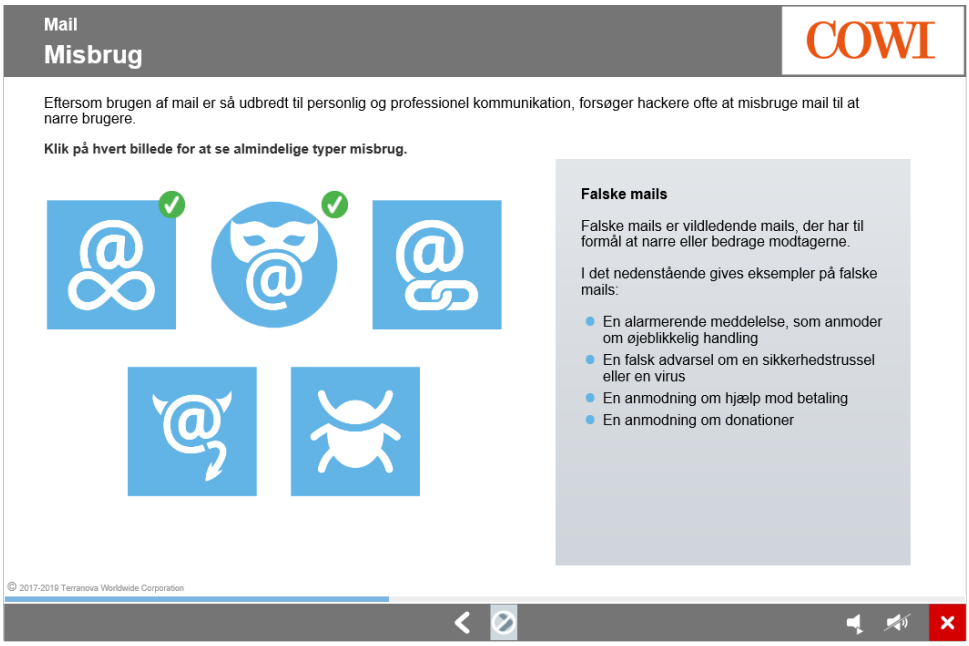
Sektion 2: Intro til e-mail (tekst-oplæsning)



Figur 6.3. Intro til e-mail (tekst-oplæsning)

I led med den næste sektion, hvor et tekststykke bliver præsenteret og oplæst, kom diversiteten af participanterne igen til kende. Her var der delte meninger om måden at præsentere indholdet på. Først udtalte P8 *„Det er sådan nemt bare at scanne sig igennem“* (J.f D:05), efterfulgt af *„Jeg trykker altid lyden af, for med lyd på så kommer det mega langsomt“* (J.f D:07). Her er det tydeligt at participanten føler sig begrænset af hastigheden på oplæsningen af teksten, og bliver lettere irriteret. Efterfølgende opstod der flere problemer relateret til oplæsningen af teksten, ikke af formen, men af indholdet. Her udtalte P8 *„Ja men problemet er her, jeg ved ikke hvad malware eller phishing er“* (J.f D:13), dette er formodentligt grundet at tekststykket benyttede begreber, som ikke var præsenteret for deltagerne endnu, og derfor kunne give problemer med at forstå den viden som blev formidlet til dem. De resterende participanter udtrykte dog stor tilfredshed med denne sektion af kurset, hvor P3 udtrykte *„Jeg synes at det er godt det er med lyd også det her med teksten her. Så kan man lige, man sidder og læser så meget her i løbet af dagen“* (J.f B:11). Denne holdning delte P4, og gav et anerkende nik dertil, og fortsatte *„Det faktisk kan være skønt lige at, hvad skal man sige, hvile øjnene en lille smule, så man får det læst i stedet for“* (J.f B:13). Denne holdning lader umiddelbart til at være delt med de resterende participanter.

Sektion 3: Vendespillet



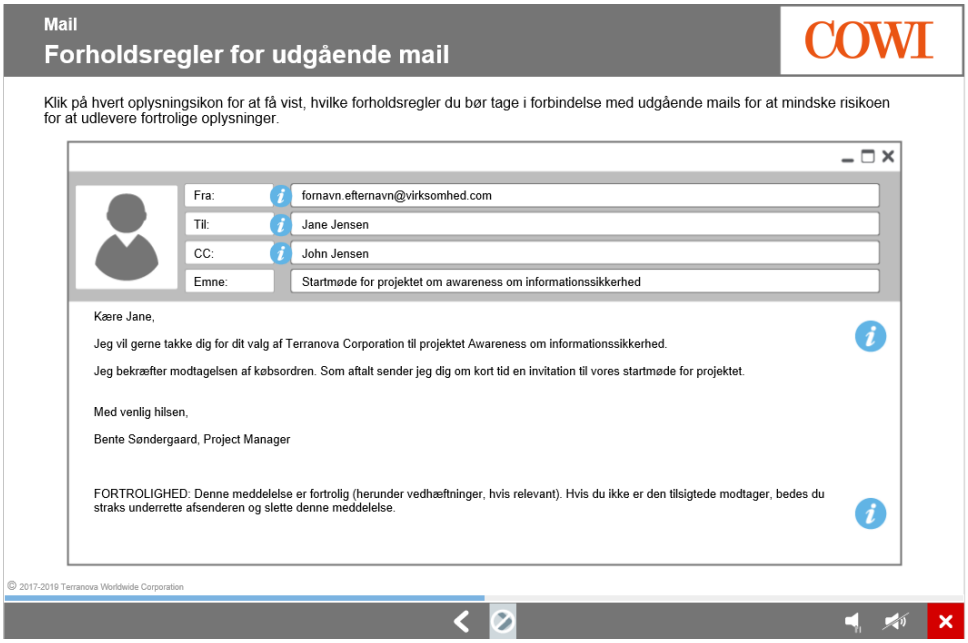
Figur 6.4. Vendespillet

I denne opgave blev participanterne introduceret for en række ikoner. Når der blev klikket på en af disse ikoner, resulterede det i at et tekststykke tilhørende ikonet blev vist, tilsvarende et vendespil. Det blev hurtigt evident at de valgte ikoner, til dels var uhensigtsmæssigt valgt, og ikke nødvendigvis signalerede den bagvedliggende mening, eksempelvis udtaler P7 *„Ja, men der synes jeg i hvert fald hvis man lige ser på ikonerne, et ikon skal man som regel kun sætte ind hvis de giver mening, og det gør de her ikke“* (J.f D:22). Generelt udtrykker flere af participanter at de valgte ikoner ikke repræsenterer den tilsvarende tekst korrekt. Trods de mangelfulde ikoner, lader alle participanterne til at være positivt stillet overfor interaktionsformen, især denne gamification, der beskriver tendensen at lave opgaver lignende spil, for at motivere deltagere, hvor opgaven i denne kontekst i høj grad kan associeres med et vendespil. P7 udtrykte yderligere en pointe med at for høj skepticisme i forhold til falske e-mails, kan spænde ben for ens reelle arbejde *„Det kommer godt nok for sådan en COWI fyr, men det kommer på engelsk, og man tænker hvorfor fanden sender han det her til mig... selvom man er kritisk, så kan man sku også blive for kritisk“* (J.f D:39). Dette kan især være problematisk i en virksomhed som COWI, der agerer internationalt, og kan have store omkostninger ved tabt arbejdsfortjeneste langsigtet, ved manglende svar til samarbejdspartnere, kunder eller kollegaer, da medarbejder sidder inaktivt og venter på besvarelser.

Ved information vedrørende falske e-mails i vendespillet, fortalte P1 om en arbejdsrelateret situation, hvor hun den forhenværende dag havde modtaget en falsk e-mail *„Heldigvis så kom e-mailen om aftenen, så tænkte jeg at jeg ikke gider logge på for at tjekke den, det kan jeg gøre i morgen tidligt. Så da jeg mødte ind næste morgen, så kom der en e-mail hvor der stod undskyld undskyld, beklager, hvis i nogensinde har trykket på det link, skal i kontakte jeres IT afdeling med det samme. Den var åbenbart helt gal“* (J.f A:14). Samtalen indikerer at falske e-mails ofte er et problem participanterne støder på i en normal arbejdssituation. Dette indikerer at de valgte emner i kurset er relevante for nuværende samfundsmæssige problemer, men også at

participanten eventuelt ville være hoppet i hvis dette havde været modtaget og åbnet midt på dagen. Ovenstående kunne indikere at kurset ikke formår at videreformidle informationen tilstrækkeligt, så den i denne kontekst ikke forstås korrekt, da participanten ikke kunne huske bedste praksis, trods at hun førhen har deltaget i kurset.

Sektion 4: Bedste praksis - E-mail visualisering



Figur 6.5. Bedste praksis - E-mail visualisering

Vedrørende kursusdelen hvor participanterne blev præsenteret for bedste praksis for e-mail, var der nogle gentagne observationer og forvirringer. Disse var blandt andet rettet mod feltet „underskrift“, hvor mange participanter var i tvivl om en fortrolighedserklæring var nødvendig, og om de havde den tilvalgt på deres egen arbejdsmail. Her udtalte P3 *„jeg tror faktisk ikke, Har vi selv sådan en disclaimer?“* (J.f B:43), hvilket afspejler forvirringen til emnet blandt participanterne. Flere af participanterne udtrykte altså stor usikkerhed overfor retningslinjer omhandlende underskriftsektionen. Her er der tilsyneladende en negativ korrelation mellem hvad der præsenteres fra IT-kursets side, og hvordan dette efterleves og forstås i praksis. Dette kunne umiddelbart skyldes, manglende praktiske informationer vedrørende COWI specifikt.

Generelt var et gennemgående tema at den formidlede information fra kurset og den egentlige praksis ikke altid var korreleret. Her udtalte P3 *„Det kan da sagtens ske at man både sender e-mails hjem til fruen og til bankrådgiveren fordi det er meget nemmere at arbejde i outlook, end at skal åbne for det der skide g-mail“* (J.f B:38). Kommentaren blev afsluttet med latter og et opsøgende blik hen mod P4, som anerkendende viste forståelse for udtalelsen. Der er altså en gensidig forståelse for, at der er tidspunkter hvor sikkerhedsforanstaltninger ikke altid bliver overholdt, til dels fordi de er upraktiske i øjeblikket.

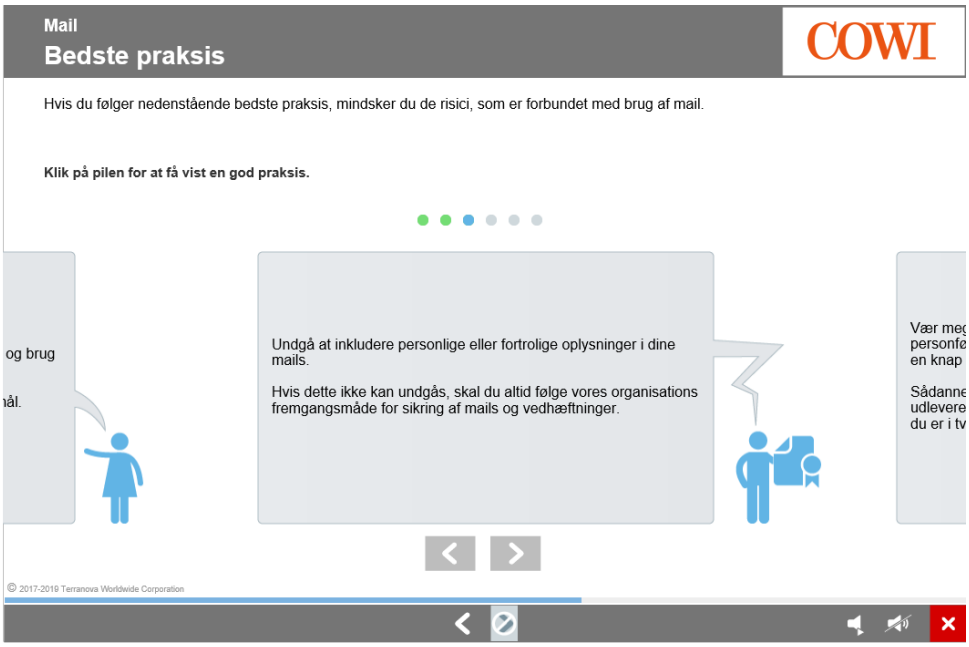
Ved præsentation af CC/BCC afsnittet vedrørende hvem der kan se e-mails, der videresendes bliver der også udtrykt en del forvirring, heriblandt P7 som kommenterede *„Nå, altså selvom de har den her informations note, så er jeg ikke helt sikker på helt hvem der kan se hvad når der bliver sendt BCC“* (J.f D:49). Dette afspejler at informationen i dette emne muligvis ikke er

fyldestgørende nok, og igen gav en mere overordnet definition på emnet, kontra en beskrivelse for hvordan anvendelse i praksis skal ske hos COWI.

I led med præsentation af emnet kryptering, blev der også udtrykt stor undren, hvilket kunne ses i en kort interaktion mellem P2 og P1, hvor P2 sagde *„Har vi mulighed for at vælge kryptering?“* (J.f A:52) og kiggede undrende på P1, hvorefter P1 himlede med øjnene og svarede leende *„Det ved jeg godt nok ikke“* (J.f A:53). Hvor der blev lagt ekstra tryk på „godt nok ikke.“ Det viser at de begge mangler information omkring emnet, og her kan der argumenteres for mangeler i kurset, der blot informerer om emner, uden at vise egentlig anvendelse af praksis for benyttelse af kryptering.

Generelt virker den nuværende praksis for e-mail til at være „mudret“ som P1 udtrykte (J.f A:41), heriblandt at deres arbejdstelefon både bliver brugt til arbejde og privat brug (J.f A:40), hvilket indikerer at der er en vag grænse for hvad der bruges til hvilket formål, og at private og arbejdsrelaterede handlinger hurtigt kan forveksles. Dette er som udgangspunkt en trussel mod sikkerheden, da de er eksponeret overfor arbejdsmæssige såvel som private angreb på deres telefoner.

Sektion 5: En gennemgang af bedste praksis for e-mail

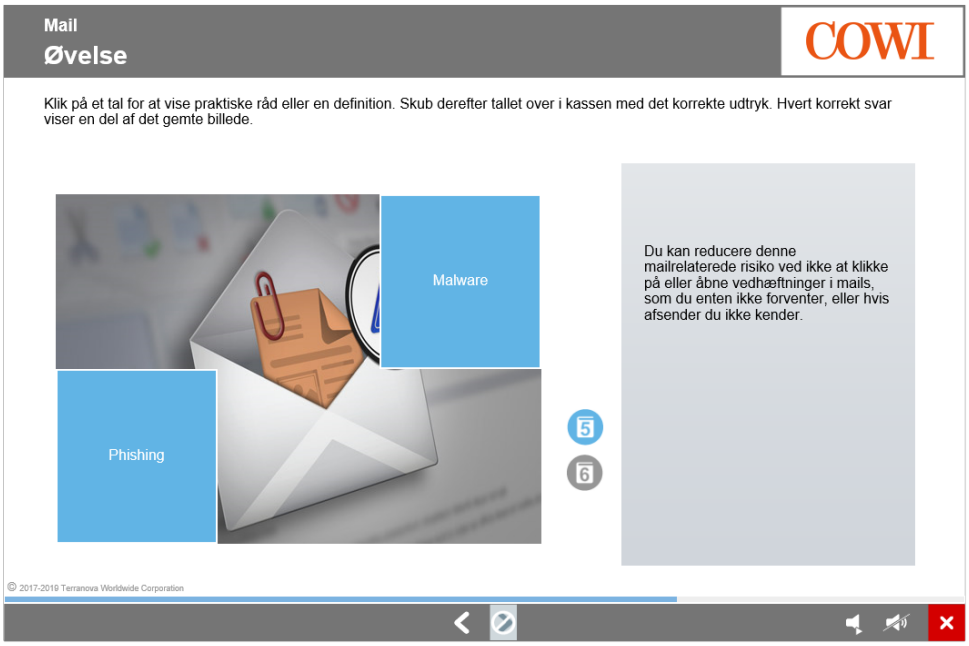


Figur 6.6. En gennemgang af bedste praksis for e-mail

Opgaven relateret til bedste praksis for e-mail, foregik relativt fejlfrit, men flere af participanterne tilkendegav dog en vis skepticisme vedrørende informationerne om den reelle brug af e-mail hos COWI, og deres evner til at overholde de præsenterede retningslinjer i praksis. Vedrørende teksten omhandlende kædebreve udtalte P6 *„Ja den der, kædebreve, det er sådan en når man sender ud til hele projekt. Så må du ikke videresende eller svare på dem, det der åbenbart mange der gør“* (J.f C:30). Dette indikerer en manglende overholdelse af denne konkrete retningslinje, til trods for at alle COWIs medarbejdere har modtaget undervisning i dette specifikke kursus indenfor det seneste år.

I led med at participanter blev eksponeret for teksten *„Undgå at inkludere personlige eller fortrolige oplysninger i dine e-mails. Hvis dette ikke kan undgås, skal du altid følge vores organisations fremgangsmåde for sikring af e-mails og vedhæftninger“*, blev der udledt en reaktion hos P2 især, hvor der blev rystet på hovedet, og kommenterede *„Jeg tror stort set aldrig at jeg sender nogle personlige eller fortrolige oplysninger“* (J.f A:65). P2 fulgte efterfølgende hurtigt op med kommentaren *„Altså personlige, altså hvad tænker man, hvor langt går man der. Om man skriver man har haft en god ferie...“* (J.f A:66) efterfulgt af en samtale omkring hvor grænsen mellem fortrolige og personlige oplysninger egentlig er. Det var er en undren flere af participanterne delte. Informationerne vedrørende fortrolige og personlige oplysninger var altså ikke noget kurset konkret svarede på, og blev præsenteret som allerede etableret viden, hvilket ikke var implicit forstået hos alle participanterne. Dette må anses som værende mangelfuld information ift. en række af brugerne, og derfor må det antages at dette burde forklares eksplicit i kurset.

Sektion 6: Puslespilsopgave



Figur 6.7. Puslespilsopgave

Participanterne blev i denne sektion eksponeret overfor en opgave, der i høj grad mindede om et puslespil. Her udtalte P8, at der var større nødvendighed for egentlig at gennemlæse teksten, da det at komme videre var afhængigt af at svare korrekt. Her udtrykte P8 følgende *„Her kan man ikke skimme, så er det hurtigere faktisk at læse det og svare rigtig på spørgsmålet første gang. Så lige på den her satte jeg mig og koncentrerede mig ekstra meget. Det synes jeg er en fordel at man skal sætte sig og læse det hele for så at svare rigtigt“* (J.f D:81). Denne kommentar bliver fulgt op af P7, som sagde *„Jamen helt sikkert, her kommer det jo til udtryk om man har forstået det man har set, hørt og læst. Så jeg synes også det er en rigtig fin måde, det inddrager en lidt mere, det gør at det enlig er noget kursusmateriale. For selvom at animationsvideoen er meget fin, så er det jo hurtigere glemt. Det her gør at man lige bliver nødt til at tænke sig om for at gøre det rigtigt“* (J.f D:82). Dette afspejler at de mere interaktive opgaver, som i høj grad minder om spil og kræver interaktion, giver bedre genkald af informationer fra opgavens indhold, og

ligeledes genvinder opmærksomheden hos participanterne. Ved korrekt besvarelse af opgaverne ses der et stigende engagementet blandt participanterne. P4 udtrykte energisk og nysgerrigt *„Ja, det er et puslespil“* (J.f B:56). Dette indikerer at kurset succesfuldt har inddraget elementer af gamification, som lader til at engagere og genvinde opmærksomheden blandt participanterne.

Ved sektionen i puslespilsopgaven vedrørende falske e-mails og phishing blev mange participanter misledt da disse to tilsyneladende mindede meget om hinanden. De svarede altså forkert, og troede at informationen omhandlende falske e-mails var phishing. Ligheden mellem disse to tekster, lod til at være høj og svær at adskille for participanterne. Det kan eventuelt forklares ved forvirrende brug af ordvalg. P7 udtrykte at phishing i teorien også er at fuppe folk, som er måden falske e-mails ligeledes er beskrevet på. Dette sluttes med en åben håndbevægelse, der udtrykte afmagt og en vis selvsikkerhed i eget udsagn.

Senere i opgaven udtrykte P7 også at opgaveteksten vedrørende phishing var forkert, da det ikke nødvendigvis var en anerkendt virksomhed som er afsender, som ellers er måden det bliver udtrykt på i opgavebeskrivelsen.

Selvom størstedelen af deltagerne var positivt stillet overfor interaktionsformen, var P5 dog skeptisk og nævnte at der var for mange „klik“ i opgaven og sagde *„det burde jo bare komme selv“* (J.f C:14), som igen vidner om diversiteten af modtagerene, som der skal tages højde for i et sådant kursus. Det var evident at op til flere participanter i led med puslespilsopgaven, i høj grad brugte udelukkelsesmetoden, for at finde frem til de korrekte svar. Det kan indikere en manglende forståelse for de konkrete tekster, hvor fokus her i højere grad er at få de rigtige svar, end at forstå den givne information.

Til sidst vedrørende information om spam, udtalte P1 *„Spam, det er også det vi har problemer hver gang vi skal lave gå hjemme møde, at vi ikke bare må sende det ud“* (J.f A:80). Dette indikerer at IT-sikkerhed skaber frustrationer til tider og kan spænde ben ift. udførelsen i praksis, hvor hun gav et eksempel i forhold til gå-hjem-møder, som skal sendes til et stort antal af mennesker i virksomheden. Hendes frustration byggede på at dette anses som spam. P2 udtrykte enighed.

Sektion 7: Sammendrag

Figur 6.8. Sammendrag

I led med det sidste tekststykke, der blev oplæst som et opsummerende sammendrag, opstod der ingen egentlige interaktioner, som udtrykte bestemte meninger om kurset eller praksis.

Sektion 8: Evaluering

Figur 6.9. Evaluering

Til sidst i kurset blev participanterne udsat for en evaluering, hvor de blev givet tre multiple choice spørgsmål, som opsummerede indholdet givet i løbet af kurset.

I led med evalueringen af kurset, var der et spørgsmål der lød *„Virus spredes så hurtigt, at jeg har pligt til at advare mine kollegaer og venner om en ny virus, lige så snart jeg bliver informeret om via e-mail. Jo flere mennesker der er klar over virussen, desto mindre sandsynligt er det at virussen“*. Hertil blev den primære del af kritikken rettet mod formuleringen af spørgsmålene, som førte til misforståelser i forhold til hvordan spørgsmålene skulle fortolkes. Dette blev observeret blandt alle participanterne, som forsagede mindre frustrationer om hvordan spørgsmålet reelt skulle opfattes. Dette kunne bl.a. ses i P7's kommentar *„Den her er nemlig åndssvag, fordi i teorien skal du selvfølgelig advare“* (J.f D:94). Dette efterfulgtes af længerevarende diskussioner som primært var vægtet i at opgaven havde misvisende information som ligeledes kunne ses i P7s udtalelse *„Opgaven er dårligt formuleret, hvis det havde været en del af dansk i skolen, så ville der have været 3 fejl i ordstillingen“* (J.f D:109). Størstedelen af participanterne mistænkte denne opgave for at være lavet med det specifikke formål at snyde dem, til at svare forkert.

I relation til spørgsmålet *„En ven sender dig en vittighed, som også indeholder en vedhæftning. Hvad bør din reaktion være?“* udtrykte P3 *„hvis det vitterligt er min ven man kan se at det kommer fra, der kan man jo tit se om det er en falske-maileller et eller andet“* (J.f B:73). Generelt blev der udtrykt en stor sikkerhed i egne evner overfor identificering af falske e-mails og eventuelle sikkerhedstrusler i e-mails. I denne kontekst afspejler det endda tilsidesættelse af nogle af kursets retningslinjer, til fordel for brug af egne forholdsregler, der potentielt kan være farligt, men dog stadig viser en konstant skepticisme, der dog i et vist omfang er sundt og et af målene ved kurset.

En kritik, der også blev rettet imod kurset, var brug af multiple choice spørgsmål. Dette illustreres af følgende udtalelse af P6 *„Jeg synes umiddelbart ikke der er noget relevans i den, hvis du bare kan gå tilbage også tage den engang mere også køre den videre indtil du har kørt på 100 procent“* (J.f C:51), hvilket ydermere førte til et løsningsforslag deraf: *„Det var måske bedre at den kom med nogle andre spørgsmål, hvis det var at man ikke havde svaret rigtigt i første omgang“* (J.f C:53).

Generelt

Til sidst tilføjede P1 opsummerende en kommentar til kurset*„Jeg mangler lidt der hvor man giver konkrete eksempler, f.eks. vores gå hjem-møder“* (J.f A:81. Dette var også en frustration, der var udtrykt tidligere enten implicit eller eksplicit, hvor konkrete eksempler mangler. Dette blev yderligere fulgt op med *„Jeg mangler nogle gange lidt at de finder på nogle ting der er konkret for mig“* (J.f A:81). Dette er en generel problemstilling, hvor konkrete COWI praksisser ikke bliver informeret om, men blot de overordnede definitioner og problemstillinger. Eksempelvis bliver der ikke informeret konkret om COWIs praksisser vedrørende krypteringer og fortrolighedserklæring, som igennem opgaverne skaber forvirring blandt størstedelen af participanterne.

Interaktionsanalyse Delkonklusion

Interaktionsanalysen hjælper med at illustrere fordele og ulemper ved den valgte form af undervisning i IT-sikkerhed. En af de primære opdagelser er diversiteten af participanterne, og dermed udfordringen ved at tilpasse kurset, så det falder i god jord hos alle. Dernæst er der også en overstående faktor, hvilket er at der er forskel på praksis og de givne retningslinjer. Dette

udmunder delvist i participanternes selvsikkerhed om egne evner, så de bevidst overtræder en række af COWIs IT-sikkerhedsforanstaltninger. Modsat overtrædes også en række af de opsatte retningslinjer, grundet uvished om emnet, såsom kryptering, vedhæftet fortrolighedserklæring i deres e-mailsignaturer og viden omkring hvad forskellen er på fortrolige og personfølsomme data. Dette er information som der informeres om i kurset, men hvor konkrete praksisser ikke bliver udspecificeret, eksempelvis fortrolighedserklæringen hos COWI specifikt. Her bliver der ofte kun givet en definition og en generel formulering af problemstillingen fra et samfundsmæssigt perspektiv som førte til mangelfuld information i en række emnefelter. Dette er også evident, ved at emner ikke kan genkaldes, som værner om relativt lav genkaldelse i forhold til at kurset er blevet udført inden for det seneste år. Det ses også ved beretninger om at retningslinjer ikke bliver fulgt, hvilket igen vidner om den relativt lave genkaldelse. I relation til de brugte ikoner ved vendespils-sektionen, kan det konkluderes at de er mangelfulde, og ikke giver øget forståelse eller indikation for emnets indhold. Op til flere participanter blev decideret forvirret, og der opstod frustration da ingen af ikonerne kunne relateres til de relevante informationer, der blev givet i led med opgaven. I relation til de anvendte fagord, var der også en vag skillelinje, mellem de forskelliges betydning, hvor beskrivelsen i høj grad var ens, hvilket igen skabte forvirring hos participanterne. Senere i kurset, er der også et specifikt spørgsmål i evalueringen, omhandlende hvad der skal gøres ved modtagelse af virus pr. e-mail. Her er participanterne forvirret i så høj grad, at de mistænker spørgsmålet for at været et „snyde-spørgsmål“, hvilket vi dog ikke kan værne om. Helt overordnet er brug af et varieret antal interaktionsformer, såsom gamification via opsætninger, der i høj grad ligner vendespil og puslespil med til at engagere deltagerne. Ydermere lader brugen af animationsvideoer og oplæsning også til at have en positiv påvirkning på engagement i kurset. Dette bliver også udtrykt op til flere gange.

6.2 Indholdsanalyse

I dette afsnit analyseres interviewdataene opnået gennem de to fokusgruppeinterviews foretaget med otte af COWIs medarbejdere. Analysen vil ske på baggrund af teorien beskrevet i afsnit 5.5. Kategorierne som analyseres er **vigtigheden af IT og IT-kurser**, **positive og negative bemærkninger vedrørende IT og IT-kurser** og **COWIs kommunikation herunder forbedringer**. Formålet med at foretage en indholdsanalyse er at få en dybere forståelse for medarbejdernes holdninger vedrørende IT-kurserne.

6.2.1 Vigtigheden af IT og IT-kurser

I COWI Aalborg ses IT som værende en essentiel del af samfundet. P1 siger om IT; *„En grundpille i dagens samfund hvis vi skal kunne eksistere som i vidensvirksomhed. Vi er utrolig afhængige af e-mails som vores primære arbejdsredskab“* (J.f E:7). Citatet, samt udtalelsen om at udvekslingen af data er mere digitaliseret i nyere tid, viser at IT og dertilhørende systemer også er essentielle i virksomheder som COWI, der behandler data fra forskellige kunder. I det udsnit af medarbejdere, der er blevet interviewet, har der vist sig en tendens vedrørende opfattelsen af IT-trusler. Opfattelsen er at de er blevet mere sofistikerede. Dette ses i citatet *„Jeg tror også det er fordi der er en forventning om at det er mere tricky. Altså der er større chance for at vi bliver fuppet“* (J.f E:32). Der er også konsensus om at angrebene sker oftere end før i tiden, dog oplever participanterne at sikkerhedssystemerne og informationerne vedrørende trusler er kommet mere i forgrunden end hvad de plejede at være. Dette bliver ytret af P1 *„Jeg tror da*

også medierne har stor, hvad hedder det, værdi i og med at det er så er i nyhederne at Mærsk er blevet lagt ned og nogle andre er lagt ned". (J.f E:134) Her drages en parallel til skandalen hos MÆRSK, som var blevet hårdt ramt af et angreb. COWI bruger IT-kurser til at informere sine medarbejdere om IT-sikkerhed. Årsrapporten, samt interviewet med Niels, afspejler at der bruges flere ressourcer på sikkerheden. De medarbejdere, som er blevet interviewet har haft varierende meninger om de givne IT-kurser. Meningen afspejles i citater såsom *„Ja det tror jeg også, jeg tror ikke at det giver det store, men jeg tror også at det er træls hvis man ikke har lært det, altså fordi man begynder lidt at tænke på det"* (J.f F:75) samt *„Altså hvis man tænker sig om så ved man jo godt at de er vigtige, men hvis man ikke har prøvet at være sat ud af spillet i en uge, så tænker man måske, at argh det sker nok ikke for mig"* (J.f E:115). Citaterne viser at overordnet har medarbejderne ikke særlig fokus på IT-sikkerheden, men at det får dem til at tænke over indholdet af e-mails. Til dette siger en af participanterne at kurserne får en til ikke at klikke på links i vildskab (F:82).
IT-kurserne ses som en erstatning for at møde i plenum, hvor en procentdel ikke modtager de nødvendige informationer. Dette udtales af en participant som siger *„Jamen jeg tænker lidt at det der IT-kursus, det er en erstatning for at vi alle sammen skal sættes ind i kantinen og sidde og høre på nogen snakke om sikkerhed i en halv time, hvor tyve procent følger med, og når vi så bliver kastet ind i kantinen lige tirsdag kl ti, så er det ikke sikkert det passer for alle sammen"* (J.f F:60). IT-kurserne ses generelt som positive tiltag hvilket vil blive forklaret yderlige i nedenstående afsnit.

6.2.2 COWIs kommunikation, herunder forbedringer

Medarbejderne oplever at COWI er hurtige til at sende informationer ud vedrørende aktuelle brud på IT-sikkerheden. Et tidligere brud på sikkerheden, som viste sig alvorligt, blev hurtigt håndteret af COWIs IT-afdeling. Til dette siger en af participanterne *„Men det var ihvertfald så græl, at de skyndte sig at sende noget ud, at hvis man havde klikket, så skulle man skynde sig at kontakte ens egen IT-afdeling med det samme"* (J.f E:45). Der er derfor ingen mangel på informationer vedrørende brud på IT-sikkerheden.

I fokusgruppeinterviewet kom det frem at der er en manglende information vedrørende antallet af IT-kurser de enkelte medarbejdere skal gennemføre i løbet af et år. Ingen af de interviewede var klar over at minimumsgrænsen ligger på tre kurser per år.
Medarbejderne beskriver nogle problematikker vedrørende IT-kurserne som hindrer forståelsen for vigtigheden af kurserne. Disse problematikker omhandler brugen af de givne informationer i IT-kurserne i forhold til specifikke projekter eller problemstillinger. Dette beskrives i citatet *„Jeg syntes der mangler lidt en opfølgning. Altså jeg syntes at der mangler at man så tager i den enkelte afdeling hvor man har nogle konkrete arbejdsområder. Altså jeg kan godt se, at hele COWI skal jo have sådan en overordnet, hvad er phishing overordnet set, men så kunne man drøfte der hvor man havde nogle konkrete eksempler."*(J.f E:72) I forlængelse med dette citat mener participanten også at COWI skal komme med en opfølgning hvor de kommer med konkrete brugskontekster som afdelingen sidder og arbejder med. Dog mener medarbejderne at IT-kurserne som informationskilder er fine, men hvis der er noget vigtigt der skal videreformidles, skal det introduceres til et af de ordinære fredagsmøder.

Ydermere ønsker medarbejderne mere information fra COWI vedrørende kurserne. Som det ser ud nu får medarbejderne en e-mail fra en anden udbyder hvilket gør dem mistænksomme og

vil derfor ikke åbne e-mailen. Dette viser dog at IT-kurserne har en effekt, da de søger at få medarbejderne til at tænke over hvilke e-mails de åbner og hvilke de ignorerer. Dette kommer til udtryk i citatet *„Det værste er at de ikke informere os om at det kommer noget. Altså jeg tænker på de her IT-kurser. Så får man en eller anden e-mail fra en eller anden udbyder, som ikke er fra COWI. Dem har jeg ikke lyst til at trykke på, og så først når den kommer op på portalen ser man det. Der synes jeg faktisk COWI glemmer noget der, idet de opfordre til ikke at åbne ukendte mails.“*(J.f E:26) En af participanterne udtaler at kurset vedrørende e-mail har en modstridende effekt, da der i en af opgaverne gives informationer ved at trykke på ukendte ikoner. Følgende citat er et forbedringsforslag til problematikken i e-mail kurset: *„Der burde komme en eller anden op ''du røg i fælden", når jeg prøver den næste ''du røg i fælden." “*(J.f F:38) Dette kan være med til at forebygge uhensigtsmæssig adgang til COWIs IT-systemer da det kan få medarbejderne til at tænke over hvilken handling de skal tage. Foruden dette problem i IT-kurset, synes medarbejderne ikke at der skal være spørgsmål med svarmulighederne sandt eller falsk. Dette kommer på baggrund af at det skrevne materiale i kurserne kan være tvetydige og svaret vil derfor være baseret på medarbejderens fortolkning af materialet. Dette kan lede til frustrationer fra medarbejderen hvilket kan resultere i at informationer vedrørende IT-sikkerheden går tabt hvilket ikke vil være i COWIs interesse. Medarbejderen udtaler *„Men man skal aldrig lave en test, hvor man skal svare sandt eller falsk, og så at det er, at det ikke er entydigt, hvad man egentlig skal svare“*(J.f F:50).

6.2.3 Positive/negative bemærkninger ved IT og IT-kurser

En af participanterne beskrev den gradvise stigning i sikkerhed på følgende måde; *„'Fra vi selv havde kontrol med vores pc'ere så er de jo gradvist ved at lukke ned for det, og det er nået dertil hvor de har lukket det så meget ned at vi ikke engang har adgang til de programmer som COWI faktisk bruger, så nu begynder det at blive så stort et problem at vi ikke kan producere i det samme omfang fordi vi skal igennem servicedesk og diverse bureaukratiske ting for at få lov at hente de mest basale programmer“* (J.f F:11). Som citatet beskriver, med opbakning blandt kollegerne, er kontrollen over medarbejdernes arbejds-pc gradvist steget. COWI har begrænset adgangen til tilladte programmer, hvilket har skabt frustrationer blandt medarbejderne. Participanten forklarer yderligere at arbejdsproduktionen er faldet, som resultat af den ekstra tid, der skal sættes af til at kontakte IT-afdelingen, og få tilladelse til at hente de ønskede programmer. Der ses altså en konsensus blandt participanterne at de nuværende sikkerhedsforanstaltninger skader produktiviteten i sådan en grad, at de har svært ved at se fordelen ved disse.

COWI Aalborg har ydermere også implementeret foranstaltninger angående selve adgangen til de brugte systemer. En af participanterne siger *„jeg skulle først tage en sms for at komme ind på computeren eller ind på nettet og så ind på Skype og så 4 sms'er, en for mail, en for Skype og så sad jeg der og jeg skulle bare ind og skrive at jeg tager kage med fordi jeg har fået baby (16:30). Så jeg endte faktisk op med bare at sende en sms til P5 og sige at du kan skrive en e-mail for jeg gider ikke.“*(J.f F:104) Som citatet beskriver, skulle participanten igennem flere barrierer for at fuldføre en simpel opgave. Denne øgede grad af sikkerhed frustrerede participanten til det punkt, at personen gav op. Dette citat, sammen med de forhenværende indikerer en øget utilfredshed blandt COWIs medarbejdere, angående de nuværende sikkerhedsforanstaltninger. Disse ses som overflødige, og disproportionale i forhold til de arbejdsopgaver, der udføres til dagligt.

En af participanterne beskriver hertil IT-afdelings handlinger som følgende *„Jeg syntes, altså ledelsen ved jeg ikke helt lige, men altså det virker som om engang imellem at COWI it (14:20) indfører noget for at holde sig beskæftiget, altså“*(J.f F:90). Som citatet beskriver, ses implementeringen af de diskuterede sikkerhedsforanstaltninger, som tiltag der laves, bare for at lave dem. Medarbejdernes samlede holdning til overfloden af foranstaltninger, har givet participanten indtrykket af at IT-afdelingen implementerer disse, uden et egentlig formål, hvilket styrker dennes opfattelse, af foranstaltningernes irrationalitet.

Der fremkommer dog også positive holdninger til sikkerhedsforanstaltningerne, som sætter sig lidt i modsætning til de tidligere udsagn *„Og det der med de koder, jamen når det bare er den ene eller to gange, så synes jeg faktisk det er rigtig rigtig dejlig. Bare sådan en sikkerhed for os hvis man skulle tabe, miste sin computer og der er en eller anden der bare lige, du kan sgu ikke logge på min computer“*(J.f F:100). Ud fra dette citat, ses der meget positivt på brugen af adgangskoder. Her udtrykker participanten den tryghed, og ro i sindet sikkerhed giver denne. Derved kan det uddrages, at medarbejderne altså ikke rummer udelukkende negative følelser for de øgede sikkerhedstiltag, men er positive overfor dem, så længe de er inden for fornuftighedens grænser, og ikke forstyrrer de daglige arbejdsopgaver i en overdreven grad.

Participanterne var generelt meget tilfredse med selve kursusformen, hvilket kommer til udtryk i dette citat; *„Det er super rart at vi kan tage dem når vi selv vil altså om aftenen eller om eftermiddagen, det er super fedt“* (J.f E:113). Her ses at participanterne er tilfredse med den frihed kursusformen giver dem. Det er nemt tilgængeligt, og de kan tage dem når de vil, og hvor de vil. I og med at de ikke skal møde op fysisk, til noget de måske ikke har interesse i, gør at IT-kurset er en tiltalende informationsform: *„Nej, jeg gad ikke læse noget selv, og jeg gider heller ikke troppe op til et møde“* (J.f E:76). Som udsagnet viser, kan et fysisk fremmøde vise sig at være vanskeligt for de fleste medarbejdere, da det skal koordineres så alle har tid.

Det at kurserne kan udføres når medarbejderne vil, gør dog også at de nemt bliver overset og de glemmer at tage dem. Dertil kommenterer en af participanterne *„Det er vel også fint nok det er uddannelse ting vi alle sammen skal tage. Remindersne synes jeg reelt set også er fine nok de er der fordi hvis det ikke var det så havde jeg glemt det“* (J.f F:149). Som det fremgår af citatet, udsender COWI beskeder, der minder medarbejderne om at de mangler at gennemføre et kursus. Disse spiller en stor rolle i at kurserne rent faktisk udføres, da de som sagt nemt bliver overset.

Participanternes holdning til det udførte IT-kursus omhandlende e-mail sikkerhed er overvejende positive, hvilket kommer til udtryk i udsagn som *„Ideen bag er jo rigtig fin“* og *„Altså jeg synes det fungerer udmærket“* (J.f E:70).

Dog forekommer der nogle kritiske kommentarer angående indholdet, og måden den givne information introduceres under kurset. En af participanterne siger følgende: *„Det synes jeg egentlig er fint. At der så er nogle elementer i det som måske er lidt kavt at man misforstår spørgsmålene så man svarer forkert, også selvom man læser spørgsmålet igen så tænker man det er jo en fejl. Så gider man ikke svare. Og jeg må først komme videre når jeg egentlig har svaret forkert. Men det kan også være vi tolker det forkert, men bare det at vi kan tolke det forkert jamen så er det jo ikke en ordentlig test“* (J.f F:29). Som det ses i citatet, henvises der til et spørgsmål i kurset, som forekommer som et trick spørgsmål. Dette skaber frustration hos participanten, i og med han svarer hvad han tror er korrekt, men som i sidste ende angives som

en fejl. Dette irriterer den samme person i en sådan grad at dette kommenteres yderligere i interviewet; *„Jamen det er fordi, for sådan nogle tests der, når jeg tager sådan nogle tests der, så irriterer det mig faktisk at der så bagefter står, du havde forkert, selvom man nok godt kunne afslutte den lidt andet. Så tog jeg den sgu lige igen, for jeg gad ikke at lukke sådan. Jeg ved ikke hvor meget COWI holder øje med os, så jeg ved ikke om der så popper op og siger, nu har du trykket forkert tre gange, om det så går ud i systemet at shit det der det er det svageste led i e-mails (10:09)“* (J.f F:52). Som det ses i citatet, er en af bekymringerne, at participanten ikke ved hvilken information COWI får i form af medarbejders kursusresultater. Dette bekymrer participanten, da denne er utilfreds med at svare hvad formodes rigtigt, men vises at være forkert. Dette betvivler personen og munder i sidste ende ud i et irritationsmoment, som deles med resten af participanterne.

Der kommenteres også på relevansen af kursusformen, hvilket ses i citatet *„Så på den måde så syntes jeg, at det, altså det er måske ikke verdenens bedste metode for at få folk til at lære det, men lige pt. så syntes jeg at det er den bedste alternative“* (J.f F:62). Participanterne er som sagt tilfredse med den nuværende platform, hvori informationen videregives, og den er at foretrække over et fysisk fremmøde, som blev beskrevet tidligere. Som udsagnet beskriver, ses kurset dog ikke som den mest optimale metode, for at få medarbejderne til at lære, og tage den information der gives til sig. Dertil kommenteres det, at et grundlag for dette kunne være at informationen, der bliver givet i kurset ses som overfladisk af nogle medarbejdere, og noget som de allerede ved i forvejen, hvortil kurset kan opleves som værende mindre relevant *„Ja men jeg tror, jeg ved ikke om den, altså, om den gør at det er mere sikkert, altså det er jeg sådan lidt i tvivl om. Der er nok nogen der lærer rigtig meget af det der, men jeg synes ikke umiddelbart der var noget i det der, der var overraskende, altså det er jo rigtig nok i beskrivelserne“* (J.f F:67). Informationen ses altså som værende meget basal og medarbejderne mangler at kunne sætte informationerne i en kontekst til deres arbejde.

6.2.4 Indholdsanalyse delkonklusion

Indholdsanalysen har fundet at IT er blevet mere essentielt, ikke bare i samfundet, men også hos COWI og deres medarbejdere. I takt med at IT er blevet mere essentielt er truslerne inden for IT stigende og angrebene er blevet mere sofistikerede. Som et modtræk til de mere sofistikerede angreb har COWI indført større sikkerhed på arbejds-pc'erne. Antallet af foranstaltninger dette har medført har, ifølge medarbejderne, formindsket produktiviteten i virksomheden. Ydermere har COWI indført IT-kurser, som skal sikre at medarbejderne ved hvordan de skal interagere med eksempelvis ukendte e-mail afsendere. Medarbejdernes holdning til IT-kurserne som et præventivt tiltag er overvejende positiv. Dog opstår der kritik til kursets indhold, med et fokus på tvetydige formuleringer. Det viste sig dog at medarbejderne ønsker bedre kommunikation fra COWIs side, hvad gælder relevansen af IT-kurserne samt hvordan kurserne kan sættes i relation til specifikke brugskontekster. Medarbejderne mener at dette eventuelt kunne komme i form af en opfølgning til kurset. Selvom kommunikationen vedrørende IT-kurserne kan være mangelfund, bliver forholdsreglerne til eventuelle sikkerhedsbrud hurtig kommunikeret ud til medarbejderne gennem intranettet.

Diskussion 7

I diskussionen vil vi tage udgangspunkt i det udførte analysearbejde i indhold- og interaktionsnalysen. Her vil vi diskutere analyseresultaterne gennem teorien fra Jaffe (J.f 4.1) og Burris (J.f 4.2). Dette er med henblik på at belyse medarbejdernes holdninger og de udfordringer, som opstår i relation til IT-kurset.

7.0.1 Diskussion ud fra Burris's teori om *computerization*

COWI har i de seneste år foretaget nogle omstruktureringer i deres virksomhed vedrørende IT-sikkerheden og implementeringen af disse. Disse implementeringer og konsekvenserne af disse kan diskuteres ud fra Burris' teori om *computerization* og indvirkningen af disse på både virksomheden såvel som medarbejderne. Omstruktureringen er baseret på ledelsens valg om at bruge IT-kurser til at informere medarbejderne om det stigende antal af IT-trusler i samfundet og hvordan disse kan forhindres. Der stilles dog spørgsmålstegn ved vigtigheden af IT-kurserne, da medarbejderne ikke kan se relevansen af IT-kurserne på baggrund af de problematikker der er vedrørende kurserne. Problematikkerne, som blev afdækket i 6.2, har hindret forståelsen for vigtigheden af IT-kurserne, da brugen af de givne informationer ikke stilles op i forhold til specifikke praksisser som der arbejdes med i virksomheden. Der kan derfor stilles spørgsmålstegn ved om omstruktureringen af virksomheden var en nødvendighed eller et forebyggende tiltag fra COWIs side. Det skal dog siges at medarbejderne kan se relevansen af IT-kurserne såfremt der forekommer en opfølgning på de givne informationer fra ledelsens side, så informationerne sættes i perspektiv i forhold til afdelinger og de projekter der arbejdes med.
Det er ikke kun IT-kurserne som COWI har implementeret for at øge sikkerheden i virksomheden. De har eksempelvis indført totrinsbekræftelse i led med indførelsen af ISO27001. Der er delte meninger vedrørende denne implementering. På den ene side giver det medarbejderne en vis ro velvidende at sikkerheden er i top såfremt arbejds pc'en mistes eller bliver stjålet. På den anden side skaber denne implementering en frustration hos medarbejderne, da der skal bruges en del tid på at komme ind i COWIs system eller hente interne programmer ned på deres computer. Dette ses som værende negativt for COWI, da; 1) frustrationen blandt medarbejderne forøges og 2) produktiviteten af hver enkelt medarbejder falder, da tiden brugt på at kontakte IT-supportere/-afdelingen tager tid ud af medarbejdernes dag, som kunne være brugt på kunderne. Foruden totrinsbekræftelsen har COWI også begrænset adgangen af tilladte programmer, hvor der er flere barrierer som medarbejderne skal igennem, hvilket har haft samme konsekvenser som ovenstående.

Ud fra ovenstående kan det derfor diskuteres hvorvidt omstruktureringen af virksomheden samt implementeringen af forskellige IT-sikkerhedsforanstaltninger er tiltag som COWI skal revurdere. I forhold til Burris' teorier om assimilering og akkomodation kan der argumenteres for at der er sket en akkomodation af IT-kurserne og implementeringen af

IT-sikkerhedsforanstaltninger på makro-niveau, da disse har ændret organisationsstrukturen. Ligeledes er der sket en akkomodation på mikro-niveauet, da det har ændret medarbejdernes dagligdag. Her har implementeringen skabt flere frustrationer end det har gavnet, hvilket har mindsket produktiviteten hos den enkelte medarbejder. I en virksomhed som COWI, hvor alle timer skal faktureres er dette et problem.

7.1 Jaffe's Tensions

I led med rapportens primære omdrejningspunkt, som værende strategisk kommunikation internt i COWI vil fokusset, i led med det konceptuelle rammeværktøj, primært være at undersøge det intraogranisationelle aspekt af COWI, herunder forholdet mellem ledelse og medarbejdere i relation til IT-sikkerhedskurset og dets virke. Denne undersøgelse vil tage udgangspunkt i den indsamlede empiri, som udspringer fra den udførte indholds- og interaktionsanalyse. Dette er gjort med hensigten om at forstå sikkerhedskursets implementering, og adskille hvad forskellen på den ønskede effekt, og den konkrete praksis er, belyst med brug af de to tensions. Dette skal dog ikke forveksles med at det interorganisationelle niveau er fraværende, blot at analyse deraf i lav grad har relevans for rapportens fokusområde, vedrørende at forstå IT-sikkerehdskurset implementering og de interne interessenters holdninger om kurset og dets succes i at formidle den givne viden til anvendt praksis. Jaffes tensions ses især relevant benyttet i en organisation, hvori den primære handelsvarer er arbejdestimer, og der derved i høj grad må fokuseres på optimering af deres primære handelsvarer, ved at fokusere på menneskelige ressourcer.

COWI er, som tidligere nævnt i casebeskrivelsen, en international organisation, som i høj grad er præget af diversitet. Dette er manifesteret i organisationens eksistens på tværs af landegrænser og ansatte med markant forskellige specialiseringer og baggrunde. Heri lader en fejlfri implementering af et IT-kursus i praksis til at være nær umulig, grundet den store forskel på medarbejderne. Her vil COWI og dets ansatte defineres som en heterogen gruppe, trods deling af arbejdsplads, titler og andre fællesnævnere. Dette værner igen om kompleksiteten af organisationen, som beskriver et yderligere behov om løbende at revurdere implementeringer i organisationen, herunder IT-kurset, som COWI har valgt at udbyde til deres medarbejdere. Heri skal det teoretiske grundlag som kurset er baseret på, ligeledes udvikles i led med identificeringer af problemer og succeser i praksisser. Dette værner i høj grad om relevansen for rapportens omdrejningspunkt.

7.1.1 Tension 1: Den menneskelige faktor

Som nævnt i teoriafsnittet (J.f 4.1) indgås der ved ansættelse en formodning fra organisationens side, om at de antagede forventninger i led med ansættelse overholdes, foruden de anførte retningslinjer i organisationen. Herunder eksisterer IT-kurset, som en af disse ansvar, der skal sørge for de ansattes overholdelse af angivne retningslinjer.

Ud fra det initierende interview med den ansvarlige for IT og herunder IT-sikkerhed, blev målet med kurset defineret som: *„det er vigtigt at jeg i videst muligt omfang får informeret om best practices til medarbejderne“* (J.f G). I led med indsamling af empiri, blev det hurtigt evident at der var en klar forskel på det tiltænkte resultat og egentlig praksis, som blandt andet ses i det følgende citat fra interaktionsanalysen: *„Det kan da sagtens ske at man både sender mails*

hjem til fruen og til bankrådgiveren fordi det er meget nemmere at arbejde i outlook, end at skal åbne for det der skide g-mail"(J.f B:38). Her afspejles det konkret at medarbejdere ikke altid følger disse retningslinjer, grundet upraktiske foranstaltningerne i led med deres arbejde. Yderligere kan uvidenhed om emnet også ligge grund for brud på de anførte retningslinjer. Dette kommer til udtryk i følgende udtalelse: *„Ja men problemet er her, jeg ved ikke hvad malware eller phishing er"*(J.f B:26). Herfra kan vi se at informationen om bedste praksis ikke havde den nødvendige indvirkning, da participanterne tidligere havde deltaget i det undersøgte kursus, og ikke havde kendskab til relevante begreber i forhold til emnefeltet. Dette understøtter også et overliggende problem i at den overleverede viden fra kurserne, ikke er lig med overholdelse af praksis og derved opnås det ønskede resultat fra ledelsen ikke. Her fra kan vi søge at forstå årsagen til denne misligholdelse, hvorvidt om det så enten er manglende motivation for deltagelse i kurserne, om kurserne er dårligt sammensat eller hvorledes.

7.1.2 Tension 2: Intergering og differentering

I relation til opvejningen mellem integrering og differentering i COWI, kan vi først erkende at COWI arbejder inden for et felt, hvor der er en række højtuddannede individer, som rent fagligt er specialiseret i forskellige felter. Dette er gavnligt økonomisk, men kan have sociale konsekvenser.

I led med indholds- og interaktionsanalysen identificerede vi flere tensions relateret til dette emnefelt. Dette udsprang fra det initierende interview i relation til mulige spændinger, som kunne være mellem ledelse og medarbejdere i relation til sikkerhedskurserne: *„Jeg tror den menige medarbejder har et mere realistisk forhold til sikkerhed, jeg tror ledelsen i COWI, som i så mange virksomheder, de vil sgu godt have det her til at gå væk"* (J.f G). I led med indholdsanalysen kunne dette i en vis grad ses afspejlet hos medarbejderne, hvori flere participanter ønskede bedre kommunikation i relation til kurserne fra ledelsens side, og generelt vidnede om manglende kommunikation herom. Dette er yderligere forklaret i det initierende interview *„man gør som ledelsen, det er klart at hvis ledelsen ikke gør det de skal, eller noget helt anderledes, som ikke at sætte password på deres telefon eller hvad fanden ved jeg, så følger resten af virksomheden"* (J.f G). Her kan der være tale om ledelsens engagement i kurserne ikke har været tilpas afspejlet, hvori medarbejderne har haft svært ved at være motiveret i kurserne af den årsag.

Konklusion 8

På baggrund af analysearbejdet samt diskussionen kan vi her udarbejde en konklusion på vores problemformulering: *Hvad er COWIs medarbejderes holdninger til deres nuværende IT-kurser, og hvilke udfordringer har disse IT-kurser medført?*

Overordnet er medarbejderne positivt stillet over for IT-kurserne som værende præventive tiltag. Samtidig er de også positivt stillet over for dets konkrete form, herunder brugen af varierende interaktionsformer. IT-kurserne ses dog som værende indholdsmæssigt mangelfulde. Yderligere er holdningen til IT-foranstaltninger overvejende negative, da de påvirker medarbejdernes produktivitet på arbejdspladsen. Dette vækker frustration hos mange af medarbejderne.

En kritik rettet mod kurserne var også manifesteret i manglende konkretisering i forhold til en arbejdssituation. Der blev her taget udgangspunkt i generiske definitioner og problemer fra et samfundsmæssigt perspektiv, kontra egentlig praksis. Det fører yderligere til lav genkaldelse af formidlet information givet under kurserne, da participanterne i høj grad ikke kunne relatere til indholdet.

En manglende motivation for kurset er set i den manglende reflektion af incitament fra COWIs ledelses side. Her er der mangel på videregivet information om relevans og værdi, når kurser udsendes til medarbejderne. Foruden dette var der en mangel på genkaldelse, til trods for at participanterne havde deltaget i kurset inden for det seneste år. Participanterne havde her problemer med centrale begreber såsom phishing og malware.

En yderligere kritik rettet mod kurset er uklare spørgsmål. Arbejdsopgaverne virkede til dels forhastede, med dårligt formulerede opgavebeskrivelser, hvor participanterne opfattede disse som "snyde spørgsmål".

Overordnet må det berettes at diversiteten på arbejdspladsen, trods flere eksisterende fællesnævnere, gør det perfekte IT-kursus umuligt. Der vil altid være udfordringer ved udarbejdelsen, grundet kompleksiteten af det menneskelige element, og forskelligheden heraf. Herfra ses det også at kursets retningslinjer i en vis grad ikke blev overholdt, muligvis grundet ovenstående faktor, hvor individer handlede på egen hånd primært grundet en af tre scenarier.

1. Uvidenhed om bedste praksis.
2. Forhøjet tiltro til egne evner inden for identificeringer af trusler, hvori retningslinjer forkastes.
3. Tilgange til IT-sikkerhed var upraktiske, og mindskede deres produktivitet.

Perspektivering 9

Rapporten sætter lys på en mikro-instans af en samfundsmæssig problemstilling, som rækker sig nationalt såvel som internationalt. Ved at tage udgangspunkt i en enkel instans af problemstillingen vedrørende kommunikation af IT-sikkerhed til medarbejdere og derved den menneskelige faktors involverering i IT-sikkerhed, kan vi få et indblik i den generelle tilstand på markedet.

Relevans og betydningen for opgaven understøttes af en generel kvantificering af organisationer fra et ledelsesperspektiv, hvori kvalitativ data let kan forkastes, da dataet er svære og dyre at analysere og indvinde. Heri kan fokusset på menneskelige ressourcer være svære at konkretisere og indsamle, som dog er vigtig, hvori den menneskelige faktor er en af de primære årsager til IT-sikkerhedsbrud.

I senere arbejde kunne det være interessant at tilgå sagen fra et mere kvantitativt synspunkt, hvor der kunne udsendes harmløse simuleringer af phishing e-mails, for at få egentlig kvantitativ data for succesen ved IT-kurser hos COWI, sågar som IT-sikkerhedskurser generelt. Heri kunne sfæren social egnineering yderligere undersøges, og herfra prøve at få en måling på eksistensen af fænomenet, skadeligheden, tilstedeværelsen og dens udspredning.

Yderligere kunne det undersøges hvordan konkrete eksempler på phising eller malware fungere på et programmeringsmæssigt niveau, og se hvilke muligheder sådan software giver, og kompleksiteten ved udarbejdelse i forhold til at omgå organisationers restriktioner i form af IT-sikkerhed.

Litteratur

Alrø, H., & Lone Dirckinck Holmfeld. (2001). *Videoobservation.* Aalborg Universitetsforlag.

Borre, M. (2017). *Rystet Claus Hjort afslører Rusland har hacket det danske forsvar over to år.* Retrieved from `https://www.berlingske.dk/politik/rystet-claus-hjort-afsloerer-rusland-har-hacket-det-danske-forsvar-over-to-aar` (Lokaliseret: 16-12-2019)

Bryman, A. (2014). *Social research methods.* Oxford University Press.

Burris, B. H. (1998). Computerization of the workplace. *Annual review of Sociology*, *Vol. 24*, 141-157.

Clulow, V. (2005). Futures dilemmas for marketers: can stakeholder analysis add value? *European Journal of Marketing.*

CompTIA. (2015). *Trends in information security study.* Retrieved from `https://comptiacdn.azureedge.net/webcontent/docs/default-source/research-reports/full-report---comptia-2015-security-study---vfinal.pdf?sfvrsn=f73b4733_0` (Lokaliseret: 01-12-2019)

COWI. (2019a). *Cowi csr.* Retrieved from `CSRhttps://www.cowi.dk/om-cowi/csr-and-compliance` (Lokaliseret: 18-12-2019)

COWI. (2019b). *Cowi hjemmeside.* Retrieved from `https://www.cowi.dk/` (Lokaliseret: 17-12-2019)

COWI. (2019c). *Cowi Årsrapport.* Retrieved from `https://www.cowi.dk/om-cowi/rsrapporter-og-noegletal` (Lokaliseret: 17-12-2019)

Cowi opgraderer it-sikkerheden. (2019). Retrieved from `https://www.nnit.dk/ArtiklerOgOfferings/Sider/COWI-opgraderer-it-sikkerheden.aspx` (Lokaliseret: 17-12-2019)

Cowi organisationsstruktur. (2019). Retrieved from `https://www.cowi.dk/om-cowi/organisation-og-ejerskab` (Lokaliseret: 17-12-2019)

Danmark Statistik. (2019). *Falske E-mails fylder i indbakken.* Retrieved from `https://www.dst.dk/da/Statistik/nyt/NytHtml?cid=28912` (Lokaliseret: 01-12-2019)

Hajer, M. (1995). *The politics of environmental discourse: Ecological modernization and the policy process.* Oxford: Clarendon Press.

Hallahan, K., Derina Holtzhausen, Betteke van Ruler, Dejan Verčič, & Krishnamurthy Sriramesh. (2015). Defining strategic communication. *International Journal of Strategic Communication*, s. 3-28.

Hestbæk Andersen, T., & Flemming Smedegaard. (2012). *Diamanten - en model til kommunikationsplanlægning.* Samfundslitteratur.

Horsbøl, A., & Pirkko Raudaskoski. (2016). *Diskurs og praksis. teori, metode og analyse* (No. ISBN: 978-87-593-1879-9). Samfunds litteratur.

Jaffee, D. (2000). *Organization theory: tension and change.* McGraw-Hill.

Koskinen, I. (2000a). Utilizing situated action perspective in usability testing. *Helsinki Razorfish*, *30*, 1391-1418.

Koskinen, I. (2000b). *Workplace studies: An ethnomethodological approach to cscw.* Retrieved from https://helda.helsinki.fi/bitstream/handle/10138/152327/Workplace_studies.pdf?sequence=1 (Lokaliseret: 01-12-2019)

Kristine Holst, H. (2018). *Ramt af hackerangreb personlige oplysninger om tusinder stjålet.* Retrieved from https://www.berlingske.dk/politik/danskernes-mest-kritiske-oplysninger-i-fare-det-er-taet-paa-en-falliterklaering (Lokaliseret: 16-12-2019)

Kvale, S., & Svend Brinkmann. (2009). *Interview. introduktion til et håndværk.* Hans Reitzels Forlag.

Kvale, S., & Svend Brinkmann. (2015). *Interview - det kvalitative forskningsinterview som håndværk* (No. ISBN: 978-87-412-6377-9). Hans Reitzels Forlag.

Marcus, S. (2018). *Ramt af hackerangreb personlige oplysninger om tusinder stjålet.* Retrieved from https://www.berlingske.dk/samfund/borger.dk-ramt-af-hackerangreb-personlige-oplysninger-om-tusinder-stjaalet (Lokaliseret: 16-12-2019)

Moore, G. (1998). *Cramming more components onto integrated circuits.* Retrieved from https://www.hte.hu/documents/10180/1032032/Moore_reprint.pdf (Lokaliseret: 12-11-2019)

Nicolini, D. (2009). Zooming in and out: Studying practices by switching theoretical lenses and trailing connections. *Organization Studies*, *30*, 1391-1418.

Raudaskoski, P., & Malene Kjær. (2016). *Diskurs og praksis. teori, metode og analyse* (No. ISBN: 978-87-593-1879-9). Samfunds litteratur.

Raudaskoski, P., & Paul McIlvenny. (2013). *Etnometodologi.* Retrieved from https://medieogkommunikationsleksikon.dk/etnometodologi-2/?fbclid=IwAR1Vjtknc_QvGQrc3rO5DdFq4Ey_hxfr0PBIryZqi2QH8enPcuqo2r3l4i4 (Lokaliseret: 29-11-2019)

Sandborn, P. (2008). *Trapped on Technology's Trailing Edge.* Retrieved from https://spectrum.ieee.org/computing/hardware/trapped-on-technologys-trailing-edge (Lokaliseret: 01-12-2019)

sikkerdigital.dk. (2019). *Professionelle angreb kræver professionel forberedelse.* Retrieved from https://sikkerdigital.dk/virksomhed/sammen-mod-cybertrusler/abena/ (Lokaliseret: 01-12-2019)

Statestik Universitet, D. (2018). *It-anvendelse i befolkningen.* Retrieved from https://www.dst.dk/Site/Dst/Udgivelser/GetPubFile.aspx?id=29448&sid=itbef2018 (Lokaliseret: 17-12-2019)

Statistik, D. (2015). *Hver fjerde virksomhed øger investeringer i it-sikkerhed.* Retrieved from https://www.dst.dk/da/Statistik/bagtal/2017/2017-06-30-hver-fjerde-virksomhed-oeger-investeringer-i-it-sikkerhed (Lokaliseret: 01-12-2019)

Statistik, D. (2017). *IT-servicevirksomheder fortsætter væksten.* Retrieved from https://www.dst.dk/da/Statistik/nyt/NytHtml?cid=28339 (Lokaliseret: 11-12-2019)

TV2. (2019). *Sommerferie-fusk: Politiet advarer imod falske mails fra din chef.* Retrieved from https://www.tv2lorry.dk/lorryland/

sommerferie-fusk-politiet-advarer-imod-falske-mails-fra-din-chef (Lokaliseret: 01-12-2019)

Universitet, A. (2015). *Kommunikation og Strategi.* Retrieved from https://moduler.aau.dk/course/2018-2019/BAKDM20188 (Lokaliseret: 17-12-2019)

Web, T. N. (2019). *Fraudsters deepfake ceo's voice to trick manager into transferring 243000 dollars.* Retrieved from https://thenextweb.com/security/2019/09/02/fraudsters-deepfake-ceos-voice-to-trick-manager-into-transferring-243000/ (Lokaliseret: 01-12-2019)

Wirth, N. (1995). *A Plea for Lean Software.* Retrieved from https://cr.yp.to/bib/1995/wirth.pdf (Lokaliseret: 01-12-2019)

Observation: hold 1 A

01. P1: Vender sig mod testperson 2

Meget pædagogisk måde at starte ud på

02. P2: Vender sig mod testperson 1 og nikker genkendende

Ja, det er det

03. P1: Gør det mere skarpt

04. P2: Mhmm

05. P1: Meget pædagogisk måde at få det på skrift og læst op, det er dejligt, nemt

[Peger på skærmen]

[Men skal vi så trykke her et eller andet sted, er der noget længere ned på skærme?]

06. P2:[Peger på skærmen]

[Ja, det må jo så være her]

07. P2: Vender sig mod testperson 1 og løfter øjenbrynene

Jaer, spam. Dem kommer der mange af synes jeg, både her og derhjemme

08. P1: Vender sig mod testperson 2, og griner

Ja, det gør der

09. P2: Falske mails, ja, populationer til en eller anden]

Vender sig mod testperson 1, og griner

10. P1: Ja også det, ja

11. P2: Dem synes jeg også der kommer mange af

12. P1: [Vender sig mod testperson 1, og gnider sig i ansigtet imens hun fortæller]

[Ja, jeg fik en den anden dag fra Danmark, der var vi godt nok helt ved at ryge på]

13. P2: Vender sig straks mod testperson 1, og løfter øjenbryn

Nåhr okay

14. P1: Heldigvis så kom den om aftenen, så tænkte jeg at jeg ikke gider logge på for at tjekke den, det kan jeg gøre i morgen tidligt. Så da jeg mødte ind så kom der en mail, hvor der stod undskyld undskyld, beklager, hvis i nogensinde har trykket på det link, skal i kontakte jeres IT afdeling med det samme. Den var åbenbart helt gal.

Bruger håndbevægelser til at forklare ovenstående, og ligger tryk på ”med det samme”

15. P2: Nåhh, var det på COWI’s mail du fik den?

16. P1: Ja det var alle der havde været i kontakt med Danmark, der lige fik den der. Og når det så kommer fra sådan en organisation

17. P2: Støtter hovedet med hånden, og vender sig mod testperson 1

Ja noget der ser specielt ud, der kommer også mange gange den der fra nets

18. P1: Nåhrr ja, dem er jeg heldigvis holdt op med at få, synes jeg

19. P2: Kædebreve, ja

20. P1: Det synes jeg ikke jeg får på mail længere, det er sådan noget Facebook noget, sådan noget kædebesked

21. P2: Ja, det er jeg enig med dig i

22. P2: [Ligger armene over kors, og sætter sig tilbage i stolen]

Svindelnumre, ja det er jo nok sådan en der fra nets f.eks.

23. P1: Joo det må det være

24. P2: Har fortsat armene over kors, og sidder tilbage i stolen

Jeg ved det ikke, der er jo nok nogen der hopper på. Jeg har bare svært ved at forestille mig, mange gange synes jeg det er dårligt dansk.

25. P1: Løfter hånden op til ansigtet og gnider sig

Ja man kan være heldigt at der er stave fejl i

26. P2: Ordstilling er underlig osv. Men det med at man skal ind og udlevere personfølsomme oplysninger, det har jeg svært ved at forstå der er nogen der gør

27. P1: Ja, men måske er det også fordi man er lidt letsindig i forhold til når man køber en masse på nettet, så tester man lige konto nummer osv.

[Ryster med hånden]

[Og hvor går grænsen?]

28. P2: Mhmm, ja

29. P1: Og jeg tænker, det kan jo ikke være ret, altså de er jo utrolige dårlige dem jeg har fået, derfor ser de nemme ud. Men jeg tænker må være let at kopiere et layout i en officiel mail, også misbruge den

30. P2: Mhmm, men det lykkes jo givetvis for nogen, ellers ville det jo ikke være så udbredt

31. P1: Nej

32. P2: Hvem var det nu det var, det var dem oppe fra Skagen. Hvad hedder de nu, Sussi og Leo, de var da blevet franarret et eller andet større beløb.

[Sætter albuen på bordet og klør sig i håret]

[Hvad pokker var det nu det var, det var da sådan noget. Det var hun meget fortørnet over, nå]

33. P2: Distribution og malware.

34. P1: Jamen det kan man jo godt nikke genkendende til alle de der fem punkter (Spam, falske mails, kædebreve, svindelnumre og distribution og malware)

35. P2: Så starter vi vel her

[Læser op fra skærmen]

[Brug altid din arbejdsmail adresse, til arbejdsrelaterede mails]

36. P2: Det sidste, skal man i hvert fald huske, der kan man nok nogen gange komme til at bruge arbejdsmailen til de personlige ting

37. P1: Ja der går det lidt stærkt engang imellem

38. P2: Det er nok mere den anden vej rundt, jeg bruger aldrig privat mail til noget arbejdsrelateret

39. P1: [Griner]

Ej ej ej, det ville aldrig ske. Nu bruger vi jo også næsten mere tid på arbejde end hvad vi gør i det private.

40. P2: Jojo, men tingene er jo også integreret f.eks. på din telefon, det er jo både en arbejdstelefon og en privat telefon der er vores mail på. Jeg har fået min mailkonto sat op så jeg kan se både mine private og arbejdsmail samme sted, selvom det er to forskellige konti. Det gør det alligevel bare lidt

41. P1: Mudret

42. P2: Ja lidt mudret

43. P1: Ja sådan har jeg det også, jeg ønskede enlig kun kalenderen. Altså så vil jeg hellere bruge 2 mailsystemer, det gør jeg enlig også, men ved et uheld engang imellem får jeg klikket så det er dem begge to der fremgår

44. P2: Ja, nå. ”Til”

[Læser op fra skærmen]

[Husk kun at sende mailen til den der er direkte berørt]

45. P1: Ja den smutter engang imellem, ser man, både når man modtager mærkeligt mails, og selv får sendt til de forkerte

46. P2: Men altså, de tænker vel også på det der med at sætte andre på cc

47. P1: Mhmm, jeg tror i det hele taget det forstyrrer folk, eller man får sendt noget ud af huset som ikke skulle have været ude, især

i de situationer hvor vi arbejder med fortrolige oplysninger såsom forsvaret, at man ikke lige får det sendt til de forkerte Frank f.eks.

48. P2: Nu står der her, at vi hvis man skal sende til flere uafhængige modtagere, så skal man overveje at bruge line copy. Altså det har jeg det sådan lidt både og med, fordi der kan også være noget værdi i at en modtager kan se, når men har jo også fået besked, ellers kan man jo risikere, at så må man hellere sendt det afsted til vedkommende, hvis han eller hun ikke har fået den. Så bliver det jo lige pludseligt dobbelt

49. P1: Jamen jeg synes også der delt ligger noget praktisk, men der er også noget kommunikation i det, at jeg lige har sat min chef cc eller en eller anden på så det er noget jeg mener alvorligt det her. Så der er også noget kommunikation

50. P1: Men andre gange, kan jeg godt se hvis man skal sende ud til en række kunder eller bydende eller et eller andet, så det selvfølgelig smart at sætte line copy på

51. P2: Enig, enig. Hvor de heller ikke har værdi på den måde

[Sidder med armene over kors, og trækker på skulderne]

[der kan også være noget fortrolighed måske]

52. P2: [Kigger undrende hen på testperson 1]

Har vi mulighed for at vælge kryptering

53. P1: Det ved jeg godt nok ikke

[Tænkepause, kigger hen på testperson 2]

bruger man ikke sådan en server

54. P2: Det ved jeg godt nok heller ikke, det kan godt være der er et eller andet kursus vi ikke har hørt efter i. Jeg har fået en eller anden mail på et tidspunkt inde fra Aalborg kommune, hvor jeg fik en eller anden mail derinde fra som jeg ikke kunne åbne. Det tror jeg måske er sådan noget krypterings noget

55. P1: Jeg ved ikke hvis man nogen ganger bruger sådan nogen servere til at uploade ting. Altså nogen gange hvis det er store, men ehh, ej det tror jeg altså ikke vi kan, fordi vi har da været i dialog med forsvaret, hvor det var problem at vi ikke måtte sende

56. P2: Ja det kan være man skal have noget særligt, sådan nogen særlige projekter, hvor man skal have servicedesk eller IT til at sætte det op på en bestemt måde

57. P1: Jaa

58. P2: [Læser op fra skærmen]

”Fortrolighedserklæring i underskrift afsnittet med angivelse af handlinger, som skal foretages, hvis mailen er blevet fejlagtigt modtaget.

59. P2: Det mener jeg jo at der står default i vores mail

60. P1: Nu er jeg lidt flov, fordi det ved jeg ikke om det gør i vores. Jeg ligger mærke til at det står i andres, men jeg tror da ikke der står at vores skal slettes

61. P2: [Det kan vi se lige her, jeg åbner lige min mail]

[Åbner mailen]

Det står faktisk hernede

62. P1: Ja det gør det da også

63. P2: [Læser op fra skærmen]

[Undgå at klikke på, downloade eller åbne vedhæftninger af mail som du ikke forventer af modtage, af en afsender du ikke kender]

Ja, det sker jævnligt. Altså at der er sådan nogen mails, selvfølgelig trykker man ikke på det

64. P2: [Læser op fra skærmen]

[Brug vores organisations mail til arbejdsrelaterede formål og bruger altid et passende sprog. Undgå at bruge din arbejdsmailadresse til personlige formål]

65. P2: [Tager hånden op til hovedet, og tænker]

Jeg tror stort set aldrig at jeg sender nogen personlige eller fortrolige oplysninger

66: P1: Altså personlige, altså hvad tænker man, hvor langt går man der. Om man skriver man har haft en god ferie fordi vi lige skulle til Thailand eller. Det er jo på en eller anden måde personligt med at man står frem til at flytte hjemmefra i 3 ugers tid.

67. P2: Men det er jo ikke sådan noget hvor man kan snige sig ind i, i et eller andet register for folks CPR numre eller adresser eller sådan noget

68. P2: [Læser op fra skærmen]

[Vær meget opmærksom overfor enhver mail som anmoder om personfølsomme oplysninger eller beder dig om at klikke på et link eller en knap i mailen. Sådanne mails bruges ofte til at narre folk til at overgive fortrolige oplysninger eller til at distribuere malware, hvis du er i tvivl er det bedst at slette mailen]

69. P2: [Vender sig mod testperson 1]

Det gør jeg i hvert fald ikke, slette mailen, det gør jeg faktisk ikke. Jeg gør tit det hvor jeg rykker den hen til den der spam/junk folder. Gør du også det?

70. P1: Ikke så tit længere faktisk, ikke efter mailen er blevet delt op i to. Jeg er faktisk ikke så tit over at kigge i alle de der nyhedsbreve og tilmelding

71. P2: Nåhr, altså dem der, der hedder ”other”?

72. P1: Jaa præcist, jeg får heldigvis sjældent, meget sjældent noget i den der. Det i sig selv føler jeg enlig har øget sikkerheden

73. P2: Man skal nogen gange bare være lidt opmærksom, fordi jeg får nogen gange i ”other”, som ikke skulle være der

74. P1: Ja det gør man, jeg går også nogen gange ind og tjekker, jeg har også fået noget for miljøstyrelsen som havnede der over. Det tænkte jeg var et nyhedsbrev, men det var så en godkendelse

75. P2: [Læser op fra skærmen]

[Du må ikke svare på eller videresende kædebreve eller falske mails, uanset hvor god grunden ser ud til at være]

Det gør vi heller ikke

76. P1: Nej

77. P2: [Læser op fra skærmen]

[Kontakt teknisk support, hvis du begynder at modtage et usandsynligt højt antal af uopfordrede mails]

78. P2: Det synes jeg ikke jeg har oplevet her, men jeg har sådan en webmail derhjemme med stofa, hvor der kommer meget skrammel

79. P1: Det oplever min forældre også desværre, men dem jeg har fungerer enlig meget godt

80. P1: Spam, det er også det vi har problemer hver gang vi skal lave gå hjemme møde, at vi ikke bare må sende det ud

81. P1: Det er faktisk der jeg synes, der kom et konkret eksempel. Jeg synes de andre er fine og man siger at spam er når man sender ud til mange. Jeg mangler lidt der hvor man giver konkrete eksempler, f.eks. vores gå hjem-møder, altså der tænker jeg jo ikke det er spam. Det er jo ikke 6kg kartofler til 24kr, det er jo nyttig viden til kunderne, men der må vi bare heller ikke sende det ud til alle. Så jeg mangler nogle gange lidt at de finder på nogen ting der er konkret for mig.

82. Moderator: Ja det var faktisk det, det synes jeg i var gode til. Jeg går lige op og slukker kameraet, også henter vi de andre ind og foretager fokusgruppe interviewet.

Observation: hold 2 B

[Video sættes på]

01. P3: [Griner]

02. P3,4: [Begge smiler ved videoens ende]

03. P3,4: [Lytter til indledning 40 sek]

04. I : Hvilke tanker har i umiddelbart om videoen, og hvad overvejelser, tanker har i om måden budskabet sendes på, måden den kommunikeres på? Er der nogle overvejelser i kommer med der?

05. P3: Jeg synes det er meget godt, at det sådan er rimelig morsomt [Griner]

06. P4: Det fanger opmærksomheden sådan der.

07. P3: At han virker sådan lidt dum ham der. [Griner]

08. P4: Ja [Griner] Ham har man ikke lyst til at være.

09. P3: Nej

10. P4: Jeg tror jeg tænkte også, nu kan jeg også huske hvordan man laver sådan noget der. Der går meget tid med sådan noget her. at man skal udfylde sådan nogle ting her. Der tænker jeg så, video er rigtig godt til at få ens opmærksomhed [Går fra at have krydsede arme, til at gestikulere mer frit] og sådan noget der. Men det tager også lang tid, man skal sidde og vente. Nu sidder vi her og venter også på at den bliver færdig og sådan noget, så det er måske også en pointe at få frem.

11. P3: [Afbryder] Nej, det er faktisk fordi vi ikke trykker videre her. Men hvad hedder det. Jeg synes også, jeg synes også at det er godt det er med lyd også det her med teksten her. Så kan man lige, man sidder og læser så meget her i løbet af dagen

12. P4: mhmmm [Nikker anerkendende]

13. P3: [Fortsætter] at det faktisk kan være skønt lige at, hvad skal man sige, hvile øjnene en lille smule, så man for det læst i stedet for.

14. I: [4 sek stilhed] Okay, lad os prøve at se hvad der sker når vi går videre

15. [ser video omhandlende misbrug, 20 sekunder]

16: I [vender sig om til test monitor] Er vi interesseret i at de skal? Ja, de skal vel løse opgaven.

16. P3: Ja [læser videre på skærmen (omkring spam)]

17. P3: [30 sek stilhed] Har du? [om at have læst færdigt]

18. P4: Ja

19. P3,4: [Læser igennem resterende kategorier 1 min]

20. P4: [Piller sig i øjet, ser ud til at kede sig lidt]

21. [stilhed 3 sek]

22. I: Hvad tænker i sådan umiddelbart, nu er det sådan lidt typisk når man sidder 2 og læser sammen selvfølgelig. men er det noget information i kan se i forvejen, eller er der noget nyt under solen, så og sige.

23. P3: Jeg tror for mig, så får man det lidt penslet ud, nogle begreber man har hørt om. Hvad der egentlig er hvad, og sådan noget der det..

24. P4: Ja, altså [2 sek pause]

25. P3: [Kigger hen mod 4]

26. P4: Ja, jeg tror sådan lige man kan ende til det meste i forvejen, der er måske lige nogle ting der. Der måske lige er, blevet frisket lidt op. ihvertfalde lige.. Hvad er forskellen på phishing og malware for eksempel, Ja, det ved man måske godt, ja altså men.

27. P4: Jeg troede for eksempel at phishing, det var de der hvor man får et link hvor man skal klikke på, jeg troede det var en phishing mail

28. I: [1 sek stilhed] Ja, det troede jeg egentlig også [griner]

29. P4: [Griner og peger på skærmen] Nej her der siger den jo at det er det der med at den ber om oplysningerne

30. I: Nåh ja, så er det nok den.

31. P3: Ja, man kan sådan lidt huske det på, det er nogle der forsøger [lader som om han fisker med hænderne] at fiske

32. P4: Ja, og fiske et eller andet.

33. I: [3 sek stilhed] Ja, vi kan egentlig bare gå videre.

34. [For læst tekst op på skærm i 20 sek.]

35. [Læser "Fra" i e-mail tekst]

Indhold af tekst: Brug altid din arbejdsmailadresse til arbejdsrelaterede mails, Du bør ligeledes ikke bruge din arbejdsmailadresse til sat sende personlige eller ikke-arbejdsrelaterede mails.

36. P3: Ja, der er ihvertfald noget praksis der

37. P4: Det går stærkt nogle gange ja

38. P3: Det kan da sagtens ske at man både sender mails hjem til fruen og til bankrådgiveren fordi det er meget nemmere at arbejde i outlook, end at skal åbne for det der skide g-mail [Griner og kigger mod 4.]

[Læser "til"-sektion]
39. P3: Ja, det er sådan… [Udtrykker enten at det er logisk at sende til rigtige mails, som man kender, eller at det ikke bliver overholdt i så høj grad, som tidligere udtrykt]

[Læser "CC/BC"- sektion]

40. P3: Ja, dem kender vi nok også til de brune der [sukker]

[Klikker videre til "indholds-sektion]

41. P3: Ja, der skal man selvfølgelig finde ud af hvad man gør, hvis man vil sende krypteret, det ved jeg faktisk ikke hvordan man gør

42. P4: [Kigger mod 3] Det gør jeg faktisk heller ikke.

[Klikker på "underskrift-sektion]

43. P3: Det der det har, rigtig mange af vores kunder sådan et eller andet nedenunder, [imitere kunde] "hvis denne mail, er sendt forkert til dig blablabla…" Men jeg tror faktisk ikke, Har vi selv sådan en disclaimer? [Kigger mod 4]

44. P4: Der står alt muligt nedenunder vores, det er ikke sådan jeg lige har læst igennem hvad der egentlig, står præcist

[Går videre til næste del af e-kursusside "bedste praksis"]

[Klikker igennem "bedste praksis"-kort 40 sek]

[Opgave om kort-placering bliver forklaret i opgaven]

45. P3: Ja, det har jeg jo lige siddet og gjort [Sætter musen ud for 4.]

46. I: Hvad tænker i om måden det er blevet præsenteret på indtil videre, er det noget der, nu skal jeg lige formulere det korrekt… Er det noget man holder ved? Er det noget som er interessant nok til at huske det måske? Det er jo svært for dig når du lige har lavet den [gestikulere mod 3] [Griner]

47. P3: Jaaa

48. P4: Jeg tænker det er godt det der, at man ikke får så meget information af gangen, ihvertfald hvor man skal klikke ["klikker på bordet"] Det har de helt sikkert også tænkt over.

49. P3: Jaa, nogle gange, der er nogle af de andre af de her kurser hvor man bare har fået [laver en omfavnelse i luften, som indikere en "stak af materiale"] sådan en dynge tekst der i hovedet, ej, det her det kommer til at tage 100 år [mimer trætte øjne, og uoverskuelighed] at komme igennem altså

50. I: Der er de lidt kortere de her videoer, eller er det bare den her specifikt [kurset]

51: P4: Jamen, også der før for eksempel, hvor man bare skal klikke, så kommer der lidt tekst og sådan

51. I: Okay, bite-sized.

52. P3: Ja, det er også det hvad skærmbilledet, ligesom, ikke indeholder alt for meget information

53. P4: Også tror jeg også, at man kan godt lide det der,[trykker på ting ud i luften] at der er nogle ting at trykke på [kigger mod 3]

54. P3: Ja

55. P4: Det er der helt sikkert også tænkt over.

56. P3: Ja, så nu sidder man sådan [gnider sine hænder sammen og mimer ivrighed] Ja, det er et puslespil

57. P4: [Griner og kigger mod 3] Ja

58. [4 går i gang med opgaven, læser i 4 sek]

59. P3: Nu ved jeg jo godt hvad det er [Griner]

60. P4: Hvorfor kan jeg ikke trække den her? [om blok på skærmen]

61. P3: Nej, det er tallet du skal trække

62. P4: Når ja

[4 svarer rigtig på 3 spørgsmål 30 sek]

64. P3: [Smiler] udspekulerede kneb, det er noget med at bruge, det er noget med at bruge fiskeredskaber

[Svarer forkert på opgave om "falske mails"]

65. P4: Nej, det er den her [Trækker boksen omkring "udspekulerede kneb hen til "falske mails"]

66. P3: Når ja,

67. P4: Phishing er der hvor man skal …. [Griner]

68. P3: Ja [Griner] jeg læste ikke det hele.

[4. Færdiggør de resterende 2 "kort" i opgaven]

[Går videre til sammendrag af kursusgang, læses højt fra skærm 46 sek]

69. P3: Så kommer der lige en test.

[Går videre til næste side med test]

70. P3: [Læser højt] en ven sender dig en vittighed via en mail, som også indeholder en vedhæftning, Hvad bør din reaktion være? Åben den og dobbeltklikke på vedhæftningen? Det vil nok være.. [smiler/griner] [4. smiler/griner] [3 Går videre til næste svarmulighed] Hvis det er en god vittighed, sender du den videre til et begrænset antal venner og kollegaer. Udfør en komplet virus scanning af din computer og underret straks teknisk support. Slet den og fortæl din ven, at du foretrækker ikke at modtage denne type mails på dit arbejde.

71. I: Tænker i nogle gange at der kan være en forskel mellem hvad man skal gøre, og hvad man réelt gør i praksis? Det er anonymt det her, skal jeg lige huske at fortælle igen.

72. P4: [2 sek tøver] [4 krydser armene, 3 krydser arme lidt efter] Altså, hvad hedder det, deeet.. [3 kigger på 4 afventende]Det er da ihvertfald sket at der kommer noget sjovt, som vi lige skal se på, flere på kontoret. Det er faktisk blevet mindre synes jeg [Kigger på 4] Der var der en gang, hvor der kom lidt sådan, øhh

73. P3: Ja, det er også svært, det kommer også sådan lidt an på [peger på skærmen med spørgsmål om mails fra bekendte] hvis det vitterligt er min ven man kan se at det kommer fra, der kan man jo tit se om det er en falsk mail eller et eller andet, og den nu ser sjov ud. Selvom den nu er fra en man kender.

74. P4: Men der er måske også noget med [1 sek pause] med hvilke filtyper som der bliver sendt, for hvis nu der er nogle, hvis der nu er nogle der sender en eller anden execute fil "prøv lige at se et eller andet sjovt" [griner]

75. P3: Ja

76. P4: Så skal man nok ikke lige, der kan selvfølgelig godt gemme sig noget inde i, hvis der er folk der sender video

77. P3: [afbryder]hvis der er et eller andet der sendt igennem facebook eller et eller andet.

78. P3: [vender tilbage til spørgsmålet på skærmen]Ja, men altså det rigtige her, at sige at man ikke vil have det. Altså den sidste mulighed der

Muligheden: Slet den og fortæl din ven, at du foretrækker ikke at modtage denne type mails på dit arbejde.

79. P3: Men altså igen, så er der lidt det der som man siger med om det her det giver dig en dårlig mavefornemmelse, for det kan jo godt være nogle der har et sjovt billede. De har været på telttur, "prøv at se det her billede" Det er jo også en vittighed kan man sige

80. P4: Ja, og så kan man jo tage fat i vennen ikke

81. [3 sek stilhed] I: Ja, men prøv at marker den i nu synes er rigtig

82. [Går til opgave 2]

Indhold: Mail er en foretrukken metode blandt hackere til distribution af malware.

83. [4 klikker meget hurtigt Sandt, og går til næste spørgsmål]

84. P3: [Læser højt fra opgave] Virus spredes så hurtigt, at jeg har pligt til at advare mine kolleger og venner om en ny virus, lige snart jeg selv bliver informeret om det via mail. Jo flere mennesker der er klar over virussen, desto mindre sandsynligt er det at virussen spredes.

85. [3 sek stilhed] I: Den er lidt tricky

86. P3: Ja

87. P4: Ja, for det er jo via mail [griner]

88. P3: Ja [1 sek pause] det er jo faktisk, ja den er nemlig tricky, fordi den er, hvad hedder det, altså jeg havde jo sagt. Så går man ud og siger det, altså for eksempel i skal lige passe på, der er en masse i omløb [peger omkring sig]altså lige de nærmeste på kontoret. Så derfor, hvis jeg nu fik en mail [gestikulere med hånden på bordet] hvor der nu var et eller andet, som jeg fandt ud af der var virus, så ville man jo ikke begynde at sende den videre. Det giver jo ingen mening. Så det de mener der, der er lige noget med. Det er selvfølgelig også fordi man skal falde i den her. Det er ikke sådan, det er ikke præcist [griner] formuleret

89. I: Så det er egentlig ikke svært at forstå budskabet, det er mere at tyde hvad det egentlig er man svarer på? [2 sek stilhed] Altså det er en lidt lang sætning, sådan lidt kludret, hvad er det egentlig de mener?

90. P4: Det får en til at tænke..

100. P3: [afbryder] peger mod tavlen, ja og også det der rent faktisk står, så siger man maan advarer sine kollegaer, men det de sådan forstår ved det, det er at man advarer via den mail man har fået. og det som man jo selv kan mene, man skal jo lige passe på hvis nu lige i andre i får den her. I skal bare ikke åbne den her [peger med fingeren] "Jeg kom til at åbne den her" [gestikulere med fingre] og nu er min computer gået i stykker og alt muligt, altså der skal man jo advare og det kan man jo også godt gøre på

mail, man kan jo starte en helt ny mail der siger, hvis i nu får noget med [1 sek stilhed]med det og det. lad det være [håndfakter der udtrykker "lad det være"] Rør den ikke, den er røget igennem vores spamfilter, det kan man jo godt gøre, altså det er sjældent man gør det fordi at man regner egentlig med at..

101. P4: [afbryder] men det er jo.. [peger på spørgsmålet]

102. P3: [afbryder igen] .. det her har de styr på, det her skal man ikke røre ved

103: I: Ja, havde du noget mere at tilføje? [Peger flad hånd mod 4]

103. P4: Nah, det var bare sådan med [snakker om spørgsmålet] man får informationer om virussen, det er jo ikke mailen der er virussen, sådan læser jeg det ihvertfald...

104. P3: Ja

105. I: [1 sek stilhed] Hvad tænker i så?

106. P4: Så skal det jo informeres ud men måske ikke lige, eller jo det kan godt være en email, men det er jo ikke den mail man sender videre, tænker jeg altså

107. P3: Nej det her spørgsmål, det er helt klart lavet at man skal falde i

108. I: Ja, hvad vil i svare så?

109. P4: Ja, sådan jeg forstår det, så vil jeg sige det er sandt [kigger på 3]

110. P3: Ja, men det vil jeg også sige

111. I: Igen, så er det ikke jer vi tester, men systemet vi tester.

112. [Klikker på Sandt, hvilket er et forkert svar, læser fejlmeddelelse]

113. P3: Den forudsætning der [peger på fejlmeddelelse] den for man ikke at vide [peger på spørgsmålet]

Observation: hold 3 C

01. P6: Griner af indholdet i vidoen

Sådan har jeg i hvert fald aldrig snakket med nogen om det på den måde der

02. P6: Reagerer på indholdet i videoen ved kommentaren

Øhh ja

Det er der vel heller ikke noget nyt i det der

03. P6: Jeg tror det egentlig er en meget fin at gøre det på med den her animationsvideo, for hvis jeg f.eks. tænker på en brochure, tror jeg at man ville lægge den væk, og tænke at den kan man altid kigge på

04. P5: Kigger anerkendende hen mod Tp6, og deler umiddelbart holdning hertil

05. P6: Spam, altså umiddelbart kan jeg ikke hvad logoet skulle have noget med spam at gøre

06. P5: Nåhr jo logoet

07. P6: Det har vi kæden, kædebrevet.

Begge testpersoner vågner op ved informationen vedrørende kædebreve

08. P6: Altså hvad synes du om den måde at sætte det op på

09. P5: Man får jo vide hvad det er og altså noget, så det er sikkert fint

10. P6: Men hvis de er så glade for at læse op, hvorfor læser de så ikke det der op os så

11. P5: Puff, det ved jeg ikke

12. P6: Nej

13. P6: Læser op fra skærmen

”Fra, brug altid din arbejdsmailadresse til arbejdsrelaterede mails. Du bør ligeledes ikke bruge din arbejdsmailadresse til at sende personlige eller ikke-arbejdsrelaterede mails”

[Jamen okay]

[Nikker for at vise forståelse af informationer oplyst i videoen]

14. P5: [Følger op på Tp5 kommentar og kropssprog ved at nikke at han forstår informationerne selv]

15. P6: Læser op fra skærmen

”Til, send kun til personer, som er direkte berørt af mailen. Dobbelttjek, at du sender mailen til den rigtige person (der kan være enslydende navne i lister)

[Nikker for at vise forståelse af informationer oplyst i videoen]

Jamen det kunne da også være dejligt

16. P5: [Jeps]

[Nikker igen for at vise at han forstår informationerne]

17. P6: Læser op fra skærmen

”CC/BCC, når du sender mails med kopi til flere personer (cc, skal du være sikker på, at mailen vedrører dem. Undgå at videresende eller sende arbejdsrelaterede mails til din personlige mailadresse”

18. P5: Der synes jeg edermanme, der er lodtrækning som

19. P6: Jaa, svar alle, ja

20. P5: [Griner for sig selv, mens han udfører kommentaren]

Der når man får den over mobiltelefonen, ser man ikke hvem der har fået den som ny

21. P6: Men altså det giver da meget godt mening, at alle vil kontrollere hvem man sender CC til. Det ville være rart med vores e-mail gruppe, men det, vores sagsmail, underscore mail, hvis man glemmer det der. Det er håbløst, også samtlige skal skrive tilbage, det har ikke noget med mig at gøre. Reply all

[Griner, da det tydeligvis er et problem at han har fået modtaget mails, der ikke har noget med ham at gøre]

22. P5: Løfter øjenbrynene til Tp6 kommentar, imens han nikker for at vise at han også er stødt på det flere gange

23. P6: Læser op fra skærmen

”Underskrift, der bør tilføjes en fortroligheds erklæring i underskriftafsnittet med angivelse af handlinger, der skal foretages hvis mailen er blevet fejlagtigt modtaget”

Har du gjort det?

24. P5: Nej det tror jeg enlig ikke

25. P6: Det kunne godt være man burde det

26. P6: Læser op fra skærmen

”Undgå at inkludere personlige eller fortrolige oplysninger i dine mails. Hvis dette ikke kan undgås, skal du altid følge vores organisations fremgangsmåde for sikring af mails og vedhæftninger”

Øhmm ja

27. P5: Men det burde jo bare være en standard at det kom med i den fortrolig mail, når de så gerne vil lave alle mulige andre standarder

28. P6: Men det må jo åbenbart være et problem, siden de ligger det ind i sådan en her. Fordi, jeg synes da ikke der er noget decideret ulogisk

29. P5: Nej nej

30. P6: Læser op fra skærmen

”Du må ikke svare på eller videresende kædebreve eller falske mails, uanset hvor god grunden ser ud til at være”

[Peger på skærmen]

Ja den der, kædebreve, det er sådan en når man sender ud til hele projekt. Så må du ikke videresende eller svare på dem, det der åbenbart mange der gør

31. P6: Læser op fra skærmen

”Kontakt teknisk support, hvis du begynder at modtage et usædvanligt højt antal uopfordrede mails”

Fedt, får lov til at ringe til internt, yess

32. P5: Speak some english

33. P5: Læser op fra skærmen

”Virus spredes så hurtigt, at jeg har pligt til at advare min kollegaer og venner om en ny virus, ligeså snart jeg selv blive informeret om det via mail. Jo flere mennesker der er klar over virussen, desto mindre sandsynligt er det at virussen spredes”

Hvad synes du?

34. P6: Griner lidt for sig selv

35. P5: Skal vi lave spam?

Griner implicit, da det er ment som en joke

36. P6: Ja mon ikke vi skal det? Det skal vi ikke. Kan du huske det?

37. P5: Om jeg kan huske det? Jeg vil da ikke begynde at sende en mail til hele firmaet bare fordi jeg har fået en virus, helt ærligt, det ville da være tåbeligt, og ville være spam

Griner

38. P6: Jamen lad os nu se, det kan da godt være

39. P5: Sådan forstår jeg det

40. P6: Så lad os da se

41. P5: Jamen det var det, kan du nok godt se

42. P6: Jamen ja

Læser op fra skærmen

”Mail er en fortrukken metode blandt hackere til distribution af malware”

43. P5: Tager hånden til hovedet, og kigger op og tænker

44. P6: Ja det må det jo næsten være, det er jo sådan set rigtigt. Fordi hvis de sender en eller mærkeligt mail med et eller andet dumt link de skal trykke på

45. P5: Ja, det kan kun være det rigtige svar

46. P6: Jaa

Læser op fra skærmen

”En ven sender dig en vittighed via en mail, som også indeholder en vedhæftning. Hvad bør din reaktion være?”

47. P5: Jeg har lyst til at tage 2’eren

Griner i led med at han ved det er det forkerte svar, men synes det er en sjov valgmulighed

48. P6: 2’eren, jaa

[Griner højlydt]

[Åben den og klikke på vedhæftningen selvfølgelig, også sende den videre]

Mon ikke bare vi skal slette den

49. P5: Men de andre vil da også gerne have den

50. P6: Ja, hold nu op det var 3 ud af 3 rigtige svar

51. P6: Jeg synes umiddelbart ikke der er noget relevans i den, hvis du bare kan gå tilbage også tage den engang mere også køre den videre indtil du har kørt på 100 procent

52. P5: Ligger hovedet på skrå og tænker over Tp6’s kommentar

[Altså man kunne jo sagtens lave spørgsmålene på en anden måde]

[Bruger armbevægelser til at forklare]

53. P6: Det var måske bedre at den kom med nogle andre spørgsmål, hvis det var at man ikke havde svaret rigtigt i første omgang.

54. Moderator: Det var ganske fint, det var det

Observation: hold 4 D

01. P8: Det synes jeg er fint det her, det gør det nemt at engagere sig i videoen

02. P7: Ja men det er altid fint at have sådan en her animation eller sådan et eller andet til at fange folk, i stedet for det bare er plain tekst. Så stilte den et spørgsmål her til sidst

03. P8: Ja, vil du åbne mailen

04. P7: Der er noget tekst

05. P8: Det er sådan nemt bare at scanne sig igennem

Bruger hånden til at illustrere at "scanne sig igennem" teksten

06. P7: Det er så spørgsmålet, om man har behov for at læse det for at kunne, om der er et element i teksten som så senere indgår i spørgsmålene

07. P8: Også trykker jeg altid af lyden, for med lyd på så kommer det mega langsomt

Kigger mod testperson 7

08. P7: Går det langsomt?

09. P8: Har du ikke hørt når den snakker?

Sidder med hånden på hagen

10. P7: Jo, kan vi ikke få lyd på her? Den er nok færdig

11. P8: Nej lyden var på, nårh ja, lad os læse

12. P7: I bund og grad, den forklarer også der hvad vi kan gøre

[Læser op fra skærmen]

"Vær opmærksom må at mail er hackers fortrukne redskab, og stol på din instinkter. Hvis en mail giver dig en dårlig fornemmelse, er der sikker noget galt. Et yderligere problem er at fortrolige oplysninger alt ofte sendes u bestykket via. Mail hvilket udgør en anden risiko"

13. P8: Ja men problemet er her, jeg ved ikke hvad malware eller phishing er. Phishing er vist vis man videresender, men malware ved jeg ikke hvad er

14. P7: Det kan være vi får at vide senere

15. P7: Ja når jeg ser sådan nogen ikoner her, så tænker jeg hvorfor have sådan nogen ikoner. Man sidder lidt om det er et vendespil. For mit vedkommende giver ikonerne absolut ingen mening

16. P8: Nej det giver ikke så meget mening, hvorfor

17. P7: [For hvis jeg nu peger på snabel a kæde heroppe, hvad er det så]

Tager hånden hen til computeren og interagerer med ikonerne

18. P8: [Ved jeg ikke, men den nederste er i hvert fald en bug]

[Peger på skærmen for at udspecificere hvilket ikon testperson 8 mener]

19. P7: Jamen er det så det? Jeg tror det er den der hedder malware

Læner sig frem og tager musen over "insekt ikonet"

20. P7: Det var det også, men er det så nu din forståelse at malware er et insekt?

21. P8: Jaer

22. P7: Ja, men der synes jeg i hvert fald hvis man lige ser på ikonerne, et ikon skal man som regel kun sætte ind hvis de giver mening, og det gør de her ikke. Selvom du nu siger at du godt kan forstå insektet her nede, men de andre for mig synes jeg ikke passer

23. P8: Den her også, det er bare en djævel

Interagere med de forskellige ikoner på skærmen

24. P7: Ja, jeg synes til gengæld det er rigtig fint at man har muligheden for at klikke ind på dem, man ved så bare ikke hvad man klikker ind på

Griner

25. P8: Nej

26. P7: Og det kan også være det er en af de her ting, med det her, at det skulle være en fælde, når man klikker på dem har man faktisk downloadet en virus, vi er faktisk nød til at klikke på den. I teorien er det faktisk forkert, vi skal klikke på noget som vi ikke ved hvad er for at få lov til at læse det

Peger på de forskellige ikoner

27. P8: Ja det er også rigtigt

Griner

28. P7: Og du kan ikke få lov til at klikke videre før du har læst det, så hvis du prøver at bestå testen kan du faktisk ikke gå videre i det. Det er i hvert fald en tanke

29. P8: Jeg læste lige dem alle sammen

30. P7: Men hvad står der så i hver enkelt. Der står vel hvad de forskellige ting er. Kædebreve, det er dem man altid ser på Facebook.

31. P8: Dem kender jeg godt

Kigger hen mod testperson syv

32. P7: Del dem her ellers lukker de din konto eller du dør af kraft

33. P8: Ja, falske mails. Så giver de nogen eksempler, det synes jeg er fint

Trykker sig videre til næste fælt falske mails

34. P8: Spam, det er vel alt det der fylder i mail boksen. Det er også fint, den fortæller os lidt at man skal passe på selv at man selv ikke kommer til at sende ud til en masse og lave spam

Kigger opsøgende hen med testperson syv

35. P7: Jeg tror alligevel man skal sende mange mails før det ses i spam

36. P8: Svindelnumre

Trykker videre gennem kurset til sektionen svindelnumre

37. P7: Jeg synes enlig det er lidt sjovt, nogen af de ting her, at vi selvfølgelig ikke skal trykke på de links vi ikke ved, men nogen gange får vi især omkring de her, uddannelsescentre og sådan nogen ting, en mail om at vi skal trykke på det link her og komme med en besvarelse

38. P8: Jaer

39. P7: Jeg kan huske omkring, jeg tror det var projectvise, så stod der hvis du er projectvise bruger, så skal du trykke her. Det kommer godt nok for sådan en COWI fyr, men det kommer på engelsk, og man tænker hvorfor fanden sender han det her til mig, også går der så 3 måneder også kommer den igen og siger du har ikke svaret. Så ser man så på kvitteringen, at den her mail skal i altså lige huske at svare på. Så det kan også nogen gange, altså, selvom man er kritisk, så kan man sku også blive for kritisk, fordi lige så snart der bare står et eller andet efter, så ved man ikke rigtigt hvordan man skal forholde sig til det

40. P8: Ja, også stoler man jo blindt på vores COWI konto, så siger vi at den er sendt for en COWI konto så den er fin, den tager vi bare

41. P7: Det er i hvert fald nemt at stole på det, hvis det er en COWI konto der står bag

42. P8: Ja, enig. Også tit kommer de på engelsk, hvor man kan sige at de masse produceret, fordi de er sendt ud til alle. Der synes jeg det er virkelig mærkeligt, jeg har lige gået igennem og slette mange af mine mails, der tænkte jeg mange af dem ser ikke ud som det almindelige format, men jeg vil tænke jeg ville trykke ind på dem alligevel fordi det er COWI akademi,

43. P7: Ja ja, jamen det er jo netop dem. Hvis man forfalsker dem så trykker man jo bare blindt på dem

44. P8: Trykker videre til næste sektion som omhandler hvilke ting man skal ligge mærke til når man sender eller modtager mails

Ja det var der hvor vi skulle kigge på information omkring dem alle sammen. Der var en ”til”, det synes jeg enlig var lidt fint, for hvad skal man kigge på

45. P7: Men her giver ikonerne f.eks. mening, at jeg skal klikke ift. at kigge på infoikonet, for at få vide hvad ”til” betyder. Der er ikke et eller andet spøjst ikon, og det giver en forståelse for hvad det er de enkelte elementer betyder

46. P8: Den her var også kort og præcist¨

Kommentar vedrørende CC/BCC

47. P7: Prøv at tage den der CC/BCC, jeg kan faktisk ikke huske den der BCC funktion der, jeg kan bare ikke lige huske, virker den som den står der? Hvis nu jeg sender en besked til f.eks. Mette Thomsen, også sætter dig på BCC, kan du så virkelig ikke se at jeg har sendt noget til Mette?

48. P8: Nej

Kigger hen med testperson otte mens hun tænker over ovenstående

49. P7: Jeg synes bare, at før hen at hvis man har været på BCC, så er det faktisk…

Peger på skærmen for at vise hvad han mener til testperson syv, imens han har en tænke pause

jamen okay så er det fordi det står forkert, eller omvendt. Jeg kan ikke lige gennemskue, altså hvis du kommer til BCC, så kan Mette ikke se jeg har sendt den til dig, men kan du så se Mettes mailadresse, det tror jeg. Nå, altså selvom de har den her informations note, så er jeg ikke helt sikker på helt hvem der kan se hvad når der bliver sendt BCC

50. P8: Klikker videre til sektion omhandlende underskrift

51. P7: Ja, det der ved jeg ikke. Den er vist standard, men det er også standard at man skal gå ind og trykke på det her link. Nederst i vores mail er der fortrolighedserklæring hvis vi ikke fjerner den som standard, så er der gå ind på vores twitter profil link, Facebook profil link, hjemmeside link plus diverse andre ting, så man får jo sådan en standard formular der i bunden

52. P8: Altså er det signaturen eller hvad tænker du?

53. P7: Jamen din automatiske signatur. Jeg har været ind og regulere i den, jeg tror ikke jeg har den med, den tekst der. Men det er også fordi jeg synes det forstyrrer billedet, nogen gange så synes jeg det bliver amerikansk tilstand at den skal lave forbehold for fremsendelse af diverse. Det kan godt være det er krav det her i dag, men det er jeg ikke klar over. Men så skal de gøre så at vi ikke kan fjerne den for vores signatur

54. P8: Min kommer ikke automatisk hvis jeg svarer på en mail, så skal jeg gå oppe og trykke signatur, så alle interne mails, så står der bare hilsen mig. Så skriver jeg bare selv

55. P7: Ja, det kan vi så lave automatisk

56. P8: Jeg har faktisk ikke fortrolighed, eller hvis det er det den kaldes signaturen, for ting jeg sender internt

57. P7: Jamen internt, så er den måske heller ikke så gal. Men ekstern ville det ikke være så godt

58. P8: Men hvis jeg åbner mailen og skal starte en ny mail, så kommer den

59. P7: Det er så fordi du har ikke været inde og redigere i den

60. P8: Jamen helt sikkert

61. P7: Det har jeg, men ellers alt i alt så forklarer det der ligesom de forskellige elementer okay

62. P8: Ja det synes jeg også, den er fin nok

63. P7: Men jeg er stadig over den overbevisning, at hvis vi begynder at lave alt det der, så skal vi ikke henvise til alle mulige internet sider på links, for det mener jeg altså den gør på basis vores signatur

64. P8: Det kan jeg ikke huske

65. P7: Jeg er også lidt i tvivl

66. P8: [Læser op fra skærmen]

[Undgå at klikke på, downloade eller åbne vedhæftninger af mail som du ikke forventer af modtage, af en afsender du ikke kender]

67. P7: Joo men altså, vi modtager jo også fra

68. P8: Fra entreprenører

69. P7: Entreprenører sender jo også en masse materiale, som du ikke nødvendigvis lige er bekendt med, og vi ved jo ikke hvor sikre deres systemer er

70. P8: Nej men så er pointen jo at man kan spørge din projektleder, om at det kan passe at vi nu har fået de her filer, hvis man ikke selv er klar over at man skal have fået dem

71. P7: Ja, man kan jo altid se indholdet om det er relevant, hvis indholdet har en relation til det man forventer. Hvis man forventer det kommer for personen, og indholdet er relevant, så må vedhæftningen jo være okay. Men det er jo altid til at vide jo, alt eksternt, deres kan jo også blive hacket, men selvfølgelig skal man have en naturlig skepsis

72. P8: Går videre til næste sektion og læser op fra skærmen

”Undgå at inkludere personlige eller fortrolige oplysninger i dine mails. Hvis dette ikke kan undgås, skal du altid følge vores organisations fremgangsmåde for sikring af mails, og vedhæftninger”

Det er det der my focus point

73. P7: Ja

74. P8: Hvor går grænsen for personlige eller fortrolige oplysninger

75. P7: Jamen det er jo GDPR relateret, og det synes jeg ikke er entydigt endnu

76. P8: Går videre til næste sektion og læser op fra skærmen]

[Vær meget opmærksom overfor enhver mail som anmoder om personfølsomme oplysninger eller beder dig om at klikke på et link eller en knap i mailen. Sådanne mails bruges ofte til at narre folk til at overgive fortrolige oplysninger eller til at distribuere malware, hvis du er i tvivl er det bedst at slette mailen]

77. P8: Ja det er lidt det samme som vi snakkede om, man bliver lagt ind i et projekt, hvor man får mail for entreprenøren. Så kan man let og hurtigt bare klikke på det link. Men jeg havde jo også forventet at det skulle komme. Det er ikke fordi jeg kender alle der arbejder i Oslo

78. P7: Nej, men generelt set skal man jo bare have en naturlig skepsis. Men man kan jo aldrig vide sig 100% sikker, fordi man ved jo heller ikke om den her afsender her er blevet inficeret af malware

79. P8: [Læser op fra skærmen]

[Du må ikke svare på eller videresende kædebreve eller falske mails, uanset hvor god grunden ser ud til at være]

Kædebreve, det er jo ikke ligefrem nået vi går så meget op i. Dem sletter vi vel ret nemt, det er vel værre med generationen over os

80. P7: Hvis der for at vores mail servere bliver presset eller sådan et eller andet, men så skal det også være nogen tunge kædebreve. Men i teorien kan det jo være, at hvis det har en vedhæftning på 1 gb og man kommer til at sende COWI all, også sender ud, så kan det godt være det bliver presset. Men det har jo ikke rigtig noget at gøre med kædebreve, det kan bare være en almindelig fejltagelse

81. P8: Så begynder vi så at lege igen, det er i hvert fald ikke noget misvisende her. Fordelen med det her, tænker jeg, at alt det andet, at videoen den har det lidt på øret, men også når vi kigger lidt på mailen, der skimmede jeg lidt. Her kan man ikke skimme, så er det hurtigere faktisk at læse det og svare rigtig på spørgsmålet første gang. Så lige på den her satte jeg mig og koncentrererede mig ekstra meget. Det synes jeg er en fordel at man skal sætte sig og læse det hele for så at svarer rigtigt

82. P7: Jamen helt sikkert, her kommer det jo til udtryk om man har forstået det man har set, hørt og læst. Så jeg synes også det er en rigtig fin måde, det inddrager en lidt mere, det gør at det enlig er noget kursus materiale. For selvom at animationsvideoen er meget fin, så er det jo hurtigere glemt. Det her gør at man lige bliver nødt til at tænke sig om for at gøre det rigtigt

83. P7&8: Bliver snydt af falske mails og phishing da de minder meget om hinanden. Altså svarer forkert, tror information omhandlende falske mails er phishing. Da testperson otte hurtigt svarer rigtigt igen efter, prøver de at trykke tilbage for at sammenligne de to tekster. Når de har svaret på alle spørgsmål, kommentere testperson otte:

84. P8: Nåhr, så bagefter kan man trykke på dem individuelt

85. P7: Ja

86. P8: Går videre til næsten sektion "Sammendrag"

87. P7: Der står stol på dine instinkter, det er jo det bedste punktum

88. P8: Går videre til næsten sektion "Evaluering"

Jeg tænkte over, jeg synes det har var nogen lidt mærkelige svar alternativer, men jeg ved hvad jeg burde svare

89. P7: Gør du det så? (Altså modtager vittigheder over mail)

90. P8: Jeg får ikke så mange vittigheder på mail, det er nok mere over SMS vil jeg tro, men jeg ved ikke helt

91. P7: Men teorimæssigt hvis du SMSer på COWI wifi

92. P8: Så ville det jo være det samme, ja

93. P8: Går videre til næste spørgsmål

Det var den her, hvor jeg faktisk tror jeg svarede forkert

94. P7: Det gjorde jeg os, den her er nemlig åndssvag, fordi i teorien skal du selvfølgelig advare,

95. P8: Ja, fordi hvis man modtager en virus så er ens instinkt selvfølgelig at advare ens kollegaer hvis de potentielt kunne have modtaget det samme

96. P7: Men det fordi den tekst er lidt misvisende, der står at ligeså snart man selv bliver informeret om det via mail, så det den enlig skriver, hvis du finder en virus skal du skrive til andre via mail

97. P8: Det er jo ikke det der står, der står bare du har pligt til at advare, ikke at du skal skrive det via mail

98. P7: Jo det står der

Peger på skærmen

99. P8: Jamen lige så snart jeg bliver informeret om det via mail, det betyder jo ikke..

100. P7: Det jo hvordan man læser ordstillingen i det, jeg læser det som om, altså i hvert fald bagefter for at prøve at forstå det, så læser jeg det som om at du informere, at du har pligt til at advare kollega og venner om ny virus om det altså via mail

101. P8: Jeg svarede i hvert fald forkert, jeg tog den to gange

102. P7: Jeg svarede også forkert, for selvfølgelig hvis der kommer en ny virus ind, så skal man skuda advare

103. P8: Jeg ville da også advare nogen, men tydeligvis ikke

104. P7: Man skal så bare ikke advare via mail

105. P8: Nej, også jo flere mennesker der er klar over virussen desto mindre sandsynlighed er der for virussen spredes. Det er ligesom sidste sætning, ja det er jeg enig.

106. P8: Mail som anmoder dig om at advare, det er jo som du siger, men det står der jo ikke i teksten, altså mails som anmoder dig,

107. P7: Nej det står der nemlig ikke

108. P8: Og falske mails, undgå at videresende det. Men det er jo ikke det den skriver

109. P7: Nej det er dårligt formuleret, hvis det havde været en del af dansk skolen, så ville det have været 3 fejl. Ordstillingen i den er forkert

Fokusgruppe 1 E

Linje nr.	Navn	Udsagn
1	M1	Jeg vil gerne starte med en præsentation så det er nemmere at transkribere, så hvis vi starter her hvor i lige kan introducere jer selv. Hvor i lige fortæller navn, alder og titel.
2	P4	Jeg hedder P4, jeg har været ved COWI i 6 år. Jeg er 32 år. Jeg sidder indenfor vand og natur, primært gjort det her
3	P3	Jeg hedder P3 og jeg er 43 og har været 12 ved Cowi. Jeg sidder også spildevandsområdet
4	P2	P2, 54 år gammel og næste år har jeg 25 års jubilæum i Cowi. Min stilling hedder vist senior projekt leder også inden for vand og miljø, promært jordforurening
5	P1	Jeg hedder P1, jeg er 48 år gammel. Jeg har været her i 20 år, så det er den tunge ende herovre. Jeg arbejder med industri-miljø
6	M1	Lige til at starte med vil jeg gerne høre hvad i forbinder med IT-sikkerhed
7	P1	en grundpille i dagens samfund hvis vi skal kunne eksistere somi vidensvirksomhed. Vi er utrolig afhængige af e-mails som vores primære arbejdsredskab
8	M1	ja, så det ligesom bliver sikkert
9	P1	ja det er vi nødt til at tro på virksomheden sætter hård ind for det skal være.
10	P3	Jeg tror jeg forbinder det med noget der er ret godt styr på i dag. egentlig med truslen, så er der flere forskellige der prøver at bombardere de forskellige systemer, svindlere og alt muligt. Men sikkerhedssystemerne tror jeg er bedre i dag end for 10-15-20 år siden. Når man kørte sin virusprogrammer på sin persolige computer, så fandt man ting og sager. Det synes jeg ikke man oplever så meget i dag.
11	M1	Så du har en forventning om der er bedre styr på det i dag?
12	P1	Jeg tror også det er fordi førhen så fik man en fysisk computer, så stod den der og så var alle tingene der, altså alt softwaren. I dag er softwaren herovre og der er ligesom en kattelem ind hvor IT så bare går ind og installere
13	P4	Man har lidt en eller anden forventning om at der er nogen der har styr på det, hvor førhen havde man sin egen computer man skulle have styr på
14	m2	Du snakker om den her kattelem, det der med IT kan tilgå computeren og rette ting. Hvordan har i det med det? Er det noget i tænker over? Er der nogle problematikker ved IT-sikkerhed som gør det kan være en dårlig ting
15	P1	Tænker du på om vi føler os overvåget?
16	m2	Ja til dels, og om der er nogle ting i skal gøre i hverdag som i føler er unormale?
17	P3	Der kan selvfølgelig godt være udfordringer med at man har alle mulig passwords til alle mulige systemer. Det nemmeste er selvfølgelig bruge nogle få passwords, selvom man får at vide man skal have unikke passwords til hver ting, men det er umuligt at huske 17 forskellige passwords, og i øvrigt skal man ændre dem hele tiden
18	P2	Jeg kunne næsten ikke få lavet et nyt password forleden, jeg skulle ændre netop til Cowis system. Men så var det en jeg havde haft for 8 gange siden eller sådan noget
19	P3	jo jo, og så finder man måske et eller andet system og det kan måske også gennemskue fordi man har nogle man ændre, man skifter rundt mellem
20	P4	Jeg tænker også at det er en overgangsfase, fordi der bliver mere og mere man skal have adgang til så må der blive opfundet nogle smartere metoder som fingeraftryk. For det er jo ikke holdbart at skulle huske 30 forskellige koder
21	P1	Det er heller ikke så længe siden at vi skulle skrive password til word, outlook og alt muligt, nu får vi bare sådan en kode, det er rigtig rart
22	M1	Hvor meget fylder IT-sikkerhed i jeres hverdag? hvis vi tænker på en arbejdssituation, primært med at overholde de reglementer som bliver giver i forhold til IT-sikkerhedkurserne. Hvor meget tænker man over truslerne?

23	P1	DEt synes jeg man tænker over. OGså fordi nu har vi har haft det kursus med gode råd til at lave et sikkert password. Og så så vi jo hvor galt det gik med Mærsk på et tidspunkt da de blev ramt. Det kostede… Det var en katastrofe, og de få gange hvor vi oplevet et brud på vores It eller et eller ande tog vi har en halv dag, vi kan intet lave, så vi er også meget sårbare på det punkt
24	M1	Ja, man er fuldstændig afhængig af at det er up to date og det kører
25	P3	Altså jeg tror ikke jeg bevidst tænker ret meget over det, men jeg har efterhånden vænnet mig til at stort set alt hvad der kommer ind af engelske mails ryger bare ud til højre også selvom det, hvad hedder det, et eller andet nyt cookie system. DEn første tanke er, nå nu er der nyt spa, ud med det
26	P1	Det væreste er at de ikke informere os om at det kommernoget. Altså jeg tænker på de her IT-kurser. Så får man en eller anden mail fra en eller anden udbyder, som ikke er fra COWI. Dem har jeg ikke lyst til at trykke på, og så først når den kommer op på portalen ser man det. Der synes jeg faktisk COWI glemmer noget der, idet de opfordre til ikke at åbne ukendte mails.
27	M1	Så det er tydeligt noget at i bliver udsat for i jeres hverdag, ift man skal have de tanker i baghoved at man ikke skal åbne de forskellige ting
28	P4	MEn det bliver man også generelt bombarderet med, så det ligge helt underbevidst, det giver sig selv mange af de her ting. Det er sund fornuft
29	m2	Føler i at det er blevet mere, eller er det samme niveau, eller måske mindre
30	P1	mere, ja
31	m2	Det er måske også naturligt efter en stigning.
32	P1	Jeg tror også det er fordi der er en forventning om at det er mere tricky. altså der er større chance for at vi bliver fuppet. tidliger de der phising mailssså var det jo dårlige oversættelser af google, hvor det var med stavefejl fra danske bank, og det griner man jo af, men på en eller anden måde så lærer de jo at stave rigtigt på et tidspunkt så kan det jo være man hopper på det.
33	M1	Ja, så de er blevet mere pålidelige
34	P3	Ja, jeg har det sådan lidt det samme, hvis ikke det kommer fra nogen man kender eller noget emne der er relevant så tænker jeg. Altså man ser jo både afsender og, når man har sin mail åben i den ene side, så man kan jo godt se det her er ikke noget jeg skal kigge nærmere på. Vi har også nogle gange nogle af vores kunder som er blevet hacket, hvor der kommer en mail fra dem, og der kommer det godt nok fra nogen man kender, men så står der noget underligt i teksten. Altså den dag hvor de ligesom kan og finde ud af hvad man ligesom sidder og arbejder med, og så sende et link eller en fil, så er vi på den. Altså hvis de virkelig kan(10:15), hvor man tænker, hold da op, nå okay, og de ligefrem skriver, nåårh og velkommen hjem fra ferie, og det hele der, havde i en god tur, der hvor man så har været henne, så hvad hedder det, så er vi på den
35	P1	Fik du en fra Danmark for nylig? for en måneds tid siden
36	P3	Ja, der var noget ja
37	P1	Ja
38	P3	Ja
39	P1	Altså der var jeg da glad for at jeg ikke lige sad og arbejdede med Danmark, fordi at det var lidt sådan en organisation man normalt stoler på
40	P3	Jo jo, ja
41	m2	I var blevet hacket eller? Eller de havde bare fået deres mail stjålet?
42	P3	Ja der kom en eller anden mail
43	P1	Ja jeg tror de, ja
44	P3	Med et eller andet mærkeligt
45	P1	Men det var ihvertfald så græl, at de skyndte sig at sende noget ud, at hvis man havde klikket, så skulle man skynde sig at kontakte ens egen it-afdeling med det samme, så
46	P2	Jeg kan da ikke huske at vi sådan for alvor har været nede at ligge herinde, har vi det? ved COWI?

47	P1	Der var engang ude på tulebakken, hvor peter høj han havde været på facebook, og han havde klikket på noget, og der blev alt kontakt til facebook cuttet fra COWI indtil, så gik der et par dage, og så fandt man ud af at det duede ikke, fordi folk de brugte det også professionelt. Kan du ikke huske det?
48	P2	nej
49	P1	Jeg var oppe på julefrokost (11:35)
50	P3	Jo men, det kan jeg godt huske, men det er godt nok mange år siden, at der sådan har været nogle øh
51	P4	Det er før min tid
52	P3	Nogle it-forstyrrelser , altså så har det allerhøjst været cockpittet der har været nede, men det er jo ikke
53	P2	Ja altså sådan nogle ting der, men ikke sådan noget sikkerhedsrelateret noget vel
54	P3	Eller portalen har været nede, altså vores egen system, men der har ikke, ikke sådan noget hvor man kan sige at det har været et eller andet ude fra der har gjort at
55	P1	Ja det ved vi jo så ikke
56	P4	Det er jo det, der foregår jo nok alt muligt vi ikke ved
57	P3	Jo jo, men, hvis det så er et angreb udefra, så er det jo ekstremt kortvarigt, altså
58	P4	Ja ja, der er ikke langt ned, før man bliver opdaget
59	M1	Men i har ligesom alle gennemført de her e-kurser før, går jeg ud fra? ja, kan i huske nogle af de emner de e-kurser kommer ind omkring? hvis i skal.. Mere sådan overskrifter i forhold til, kan i huske nogle af de ting?
60	P2	GDPR har vi haft
61	P4	Også den med passwords
62	P1	Ja. Der må være en til, var der ikke fire i sidste?
63	P3	Ja så den her, med sikkerhed
64	P2	E-mail
65	P3	E-mail ja
66	P1	Det var tre, var der ikke fire den sidste runde?
67	P2	Der Var også sådan med terror, eller sådan noget der kommer udvedkommende ind, at der bare bliver lukket en tekniker ind til printeren, og sådan nogle ting. Jeg kan egentlig ikke huske hvad overskriften på den var
68	P1	Nej
69	M1	Men hvad tænker i om måden i bliver introduceret til de her tiltag, til de har e-kurser på. Syntes i det fungerer på en god måde? Syntes i det fungerer mindre godt, eller hvad tænker i forhold til den måde i ligesom bliver introduceret til det på
70	P2	Altså jeg syntes det fungerer udmærket
71	P3	Ja
72	P1	Ja det er meget let tilgægeligt. Jeg syntes der mangler lidt en opfølgning. Altså jeg syntes at der mangler at man så tager i den enkelte afdeling hvor man har nogle konkrete arbejdsområder. Altså ejg kan godt se, at hele COWI skal jo have sådan en overordnet, hvad er phising overordnet set, men så kunne man drøfte der hvor man havde nogle konkrete eksempler. Altså netop igen det der vores gå hjem møder, vi ikke bare må sende mails ud til alle kommuner, med at vi holder det her møde (13:50). Men at vi er nød til at sende dem personligt og sådan noget, for at vi ikke falder i sådan nogle grupper hvor man tænker at det her er ikke spam for mig, men det er jo så i hvad skal man sige, lovens forstand. Så der syntes jeg vi mangler at følge op på det på hvordan, med de opgaver vi sidder og arbejder med. Hvad er det så for nogle konkrete eksempler
73	M1	Ja sådan, i forhold til den afdeling man sidder i

74	P1	Ja
75	M1	Ja det giver god mening. Hvis man tænker på det her med, hvordan i bliver informeret om it-sikkerhed, kunne i så forestille jer nogle andre måder man kunne informere om it-sikkerhed på
76	P1	Nej, jeg gad ikke læse noget selv, og jeg gider heller ikke troppe op til et møde
77	P2	sådan et fredagsrundstykke møde?
78	P1	Ja, der syntes jeg man skulle tage det i konkrete eksempler, men ikke sådan helt undervisning
79	P3	Altså nej, som kurser tænker jeg heller ikke, altså så skal det virkelig hvis der er et eller andet helt vildt græl, som man bare vil slå fast med syv tommer søm så, så kan man jo introducere til det på sådan et almindeligt fredagsmøde. Men sådan hvad kan man sige, almindelig undervisning som alla det her, så tænker jeg at det her er en fin form, der også gør at man kan, altså at man kan gøre det
80	P4	At man er tvunget til at gøre dem, det er jo også ret (hvad? 15:07)
81	P3	ja ja, og man kan gøre dem på et tidspunkt der passer en. Der er lidt forskel på de kurser, fordi de her kurser omkring sikkerhed syntes jeg faktisk har fungeret fint, men det der omkring GDPR, og nogle af de der ting, det syntes jeg det var, altså det kunne jeg ligeså godt have undværet næsten. Måske var emnet også lidt mere kedeligt men øh
82	m2	Var det fordi det var kedeligt? eller fordi det var let? eller svært? eller hvorfor?
83	P3	Det var kedeligt, og så fandt man faktisk ikke helt rigtigt ud af hvad det egentlig var man skulle gøre i praksis, fordi det var sådan et generalt kursus, som nok i virkeligheden var lidt for generalt. De her ting er selvfølgelig også generelle, men det er også bare naturligt at de er generelle, men jeg syntes bare ikke vi bliver klogere på hvad vi så skulle på vores projekter, i de der GDPR kurser
84	P2	Nej det var måske lidt for tidligt, at vi fik lavet kurserne i forhold til at få
85	P3	Det kan også være
86	P1	Jeg syntes det er fint nok at de highlighter at der er noget der hedder GDPR, og man skal passe på, men jeg blev heller ikke en døj klogere
87	M1	Så der var ikke rigtig nogle specifikke retningslinjer som fortalte, bang bang bang, sådan her skal det gøres
88	P3	Neej
89	P4	Kun sådan overordnet, ikke sådan hvordan vi skulle gøre det på projekterne
90	P2	Ja, det er jo overordnet ja. Var det ikke også der, der var de der flow diagrammer, og hvis det var sådan så skulle vi gøre det der
91	P4	Hvordan gør vi det i Kosystemet(16:37) det står der ikke noget om
92	P1	Nej der syntes jeg man er nødt til at tage det i de enkelte afdelinger, og så tage nogle projekter og sige, sådan bør vi gøre, og det er denne her type data. For jeg tror heller ikke vi tænker over hvad det er for nogle type data vi ikke må have
93	M1	Nej
94	P1	Det er så nemt at have et navn til at stå og telefonnummer. Er det GDPR?
95	M1	Ja, ja
96	m2	Er det sådan på jeres e-mails at der er sådan nogle linjer med at det her må i ikke, eller der er noget med (kan ikke høre hvad der siges 17:00)
97	P4	Står der sådan noget i vores?
98	P2	Jeg tjekkede lige vores mails her, og der gjorde i min
99	P4	Okay, for der står en helt masse
100	P2	Det gør der i min ihvertfald, men det gør der ikke i Hannes
101	P1	Der gjorde ikke i min, så jeg skal da op og se om jeg ikke kan opdatere den

102	P2	Jeg tror måske bare du skal opdatere din mail, for jeg tror ikke jeg har lavet noget særligt
103	M1	Syntes i de her e-kurser de er fyldestgørende? nu hører jeg jo lige hvad i siger om GDPR kursus, at det har ikke været så fyldestgørende, men sådan rent generelt hvis vi tænker på de her kurser, altså føler i der er noget information i mangler? Får i den information der ligesom skal være til rådighed?
104	P4	Tit så kommer det uden man egentlig ved hvad formålet er. Vi ved ikke hvad COWI vil opnå med det altid, så hvis det bare er at fortælle hvad GDPR er, så er det måske fint nok, men hvis de gerne vil fortælle os hvordan vi skal håndtere det, så er det ikke godt nok
105	P3	Altså man kan jo sådan lidt, altså det der selvfølgelig er, at de er upersonligt på den måde, at man ikke, at man tænker dem nok mere vejledende end at hvis nu ens sektionsleder, eller en anden går hen og rusker i en ''det her skal du simpelthen huske'' eller det skal du efterleve. Der bliver det sådan lidt mere vejledende, arh okay vi skal også lige huske, og jaja vi må ikke sende en sjov mail til kollegaen eller hallo, men det gør vi alligevel
106	P2	Måske gør du det fra COWI til COWI
107	P3	Jeg har også fået rigtig mange fra invidan(hvad 18:50)
108	M1	Ja, føler i de her kurser er vigtige eller er en ting man bare gør fordi man skal? det er måske også at sætte det lidt op sort på hvidt, men mere sådan
109	m2	Men det er annonymt
110	P2	Ja, det sidder jeg også bare og tænker
111	P1	Ja vi ved jo godt man skal, men jeg var da nok fire dage over sidste gennemførselsdato
112	P3	Sidste salgsdato
113	P1	Ja, sidste salgsdato. Det er super rart at vi kan tage dem når vi selv vil altså om aftenen eller om eftermiddagen, det er super fedt, men det gør også bare det, at det er altid det der bliver skubbet, fordi man er altid bagud med arbejdet
114	M1	Ja så er der selvfølgelig nogle andre ting der presser på
115	P2	Altså hvis man tænker sig om så ved man jo godt at de er vigtige, men hvis man ikke har prøvet at være sat ud af spillet i en uge, så tænker man måske, at argh det sker nok ikke for mig
116	M1	Ja, de her e-learnings kurser, hvis i skal tænke på sådan en normal arbejdshverdag, hvad i ligesom går rundt og laver. Hvor stor en indflydelse tror i I har, i forhold til at hvis vi ser på det her med emails. Hvor meget tænker i over sådan
117	m2	Det tror jeg lidt vi har været inde på
118	M1	nårh ja
119	m2	Ja
120	M1	jo, men det har vi
121	m2	Det er mere i forhold til tiden
122	M1	Så kører vi lige videre. Føler I at de IT-sikkerhedsmæssige tiltag har en stor rolle i hverdagen? Altså de her kurser i bliver introduceret for?
123	m2	I er sgu gode til at snakke
124	M1	Føler i at i skal være opmærksomme på såsom phishing og malware der bliver sendt? Det har vi jo som sådan
125	P2	Jamen det gør vi da. Det tror jeg måske nok også vi er. Det har vi da nok alle sammen.
126	P4	Der kommer mere end der har gjort
127	P3	Ja, der er kommet en del igennem her på det sidste
128	P2	Vi snakkede lidt (peger på P1), det var dig der nævnte det der at efter vores e-mail bakke er blevet delt op i (21:16), så er der måske nogle ting vi ikke ser mere som bare ryger over i den der odder der så gør vi ikke noget ved det.

129	P3	Næ, men så kommer der alligevel nogle over i inboxen også
130	P2	Jamen det gør der
131	P3	Men jeg synes man hurtigt, altså når man har været inde i så mange år, så synes jeg hurtigt man spotter hvad det er man ikke skal røre ved, altså..
132	P2	Men det er nu også fordi det ligger sådan i baghovedet ikke også. Nå ja så tænker du det skal jeg ikke røre ved, det skal væk. Sådan rutienret
133	P3	ja
134	P1	jeg tror da også medierne har stor, hvad hedder det, værdi i og med at det er så er i nyhederne at Mærsk er blevet lagt ned og nogle andre er lagt ned og Frk. Jensen har indbetalt til aftenkassen måske. jeg tror da at derigennem bliver man da også mindet om
135	P2	Vores.. Et af vores laboratorier var jo også helt væk i 14 dage hvor de slet ikke kunne kommunikere med nogen som helst nærmest
136	P1	wow
137	P2	Ja, det var godt nok slemt
138	P1	Ja
139	m2	Var det COWI eller.
140	P2	Det var et laboratorie vi har, nogle der hedder Eurofins
141	m2	Nå, ja
142	P2	Så. Jeg ved ikke hvad det var der var sket, men de kunne i hvert fald ikke levere nogen som helst analyse rapporter og mails kunne de heller ikke nogle dage.
143	P1	Det lyder dyrt
144	P2	Ja
145	m2	Er der steder hvor det ikke kun går ud over e-mails? For eksemepel med det laboratorie, er der steder hvor der også er noget man skal bekymre sig om hos COWI i forhold til IT-sikkerhed, altså fysiske IT-sikkerhed. Nu ved jeg ikke helt konkret hvad det er i sidder med af maskiner, men er der noget som ikke er e-mail som er sådan noget man også skal være varsom overfor?
146	P2	Ja, det er der .
147	P1	Nogen der stjæler noget eller?
148	m2	Mest ovre i IT-genren, men..
149	P2	Vi kan jo have udveksling af filer for eksempel
150	m2	Ja
151	P2	Med kunder. Der har vi jo sådan nogle forskellige platforme hvor, ja jeg har ikke brugt det særlig meget..
152	P3	Ja, der er jo forskellige webbaseret platforme hvor man arbejder. Jeg arbejder meget på en platform hos nogle kunder, men man kan sige at man har nogle indkrænkelser, at de i hvert fald er beskyttet af at de har oprettet en som bruger og man har password og det ene og det andet. nogle gange kan det godt ret tungt at komme ind igennem det, de der firewalls for at.. Men ja, jeg ved ikke rigtig hvad risikoen ved det er fordi man har jo ligesom to parter som har godkendt hinanden i forvejen eller man har inviteret til og vi har jo også nogle af vores projekter som vi også godt kan have eksterne folk på vores projekter som kan ligge noget op på vores, et af vores portalsites og jeg ved simpelhent ikke om hvad risikoen er
153	P2	Det tror jeg da også godt man kan, men der er for eksempel også det der Dropbox
154	P4	Ja, der er ikke muligheder for at udveksle.
155	P3	Nej
156	P2	Det må vi sådan set ikke bruge i COWI hvis det er rigtig, fordi det er åbenbart ikke vurderet til at være sikkert nok
157	P3	Men det kan være svært
158	P2	Men der er nogen af vores kunder som gerne vil bruge det, hvad gør man så?

159	P1	Ja
160	P4	Der er google drive. Der er mange af dem hvor det ikke altid er den løsning vi skal bruge der er den nemmeste og det er måske en udfordring nogle gange.
161	P3	Det kan være svært
162	P4	Det kan være svært at få det udenom og så bruge noget der er nemmere, men ikke godkendt.
163	P3	Det kan være svært at få, hvad hedder det, fotos fra sit kamera over på computeren hvis ikke man lige har fået sin ledning med, så er det nemmeste jo lige at bruge Dropbox.
164	m2	Ja
165	M1	Ja
166	P3	Altså man kan godt sendte et billede, men hvis nu man har 17 billeder, man har været ude på et eller andet tilsyn et eller andet sted så kan man jo ikke sende dem i e-mail. Det er umuligt med de kameraer i dag.
167	P2	Det er nogle store e-mails du har. Men det synes jeg også fylder lidt nogen gange, det der med udveksling af filer.
168	P1	Ja
169	m2	02:37 ligesom med passwords.
170	P3	Der er selvfølgelig også sådan noget usb drev og sådan noget. Det er ikke så meget vi bruger det som vi gjorde engang tænker jeg ikke. Men altså, ja der er da noget
171	P4	Vi bruger mere og mere det der med udveksling digitalt. Tag en entreprenør som skal have en afsætningsfil, så bliver der lavet et eller andet alt mulige forskellige drevs. Sådan at de hele tiden kan tilgå den nyeste
172	P1	er det så på COWI portalen
173	P4	Det er lidt forskelligt. Nogen gange på den der eksterne COWI portal, men det kan også være et eller andet FTB-server
174	P1	Har vi så nogle retningslinjer i COWI for hvad vi må bruge?
175	P4	Ja
176	P1	okay
177	P4	Eller der er ligger, eller vi har faktisk et sted inde på IT-portalen hvor vi kan se, der er de her muligheder for udveksling. Den kan have så meget og den anbefaler vi og sådan noget der i forhold til sikkerhed og..
178	P1	nå
179	P3	Jo men altså er du nu ude og skal holde et indlæg og det er din computer som er den der bliver brugt til at vise noget fra så kommer der de fire andre indlæg, så kommer de med hver deres USB-pind og smider på din computer.
180	P4	Scanningen hopper du lige over
181	P3	Hvis de havde været i god tid så sender de det. Hvis det er kvinder så sender de det dagen.. Så sender de det en uge i forvejen. Hvis det er mænd så kommer de med et USB-stik fordi de lige har siddet og forberedt det til de første indlæg, gjort deres indlæg færdig.
182	M1	Tager i selv nogle initiativer til at opretholde IT-sikkerheden. Det kan både være i det private, når man ligesom er hjemme eller når man er på arbejdet. Et eksemple på det, lige hurtigt, det kunne for eksempel være at man tog mere end de tre tilladte sikkerhedskurser som man skal gennemføre om året hvis i kunne tænke på nogen initiativer i selv foretager i forhold til IT-sikkerhed
183	P3	Jeg tør ikke lave backup på.. I en sky eller.. Jeg har det hele på harddisk eller på to harddiske fordi man har jo også et, det er nok min største bekymring, det er hvis det skal forsvinde alt de der fotos og alt det der man har. Ikke lige så bange for at det der skulle blive stjålet, det er mere det der med at det skulle forsvinde ved tyveri eller brand
184	P2	Så skal du bare huske at have computeren med ud
185	P3	Der er for meget til at det kan ligge på computeren

186	P4	Har du så både i skyen..?
187	P3	Nej, jeg har ikke noget i skyen. Jeg gider ikke betale for det. Det er arbejde vi snakker om.
188	P4	Det her er meget nemmere.
189	P3	Ja ja jeg har bare ikke lige fundet ud af hvordan man gør uden at betale for det.
190	P1	Der er sikkert nogle hjemmesider der er gratis, men så tror jeg ikke jeg vil lægge mine ting der
191	P4	Nej, man betaler vel også for et eller andet.
192	P1	Ja, det må man håbe.
193	m2	Jeg kan anbefale google drive hvis det er. Ja, har vi mere?
194	M1	Nej det var egentlig de spørgsmål, medmindre du har mere?
195	m2	Nej ikke umiddelbart.
196	M1	Jamen så var det det. Igen tusinde tak fordi i gad at deltage og bruge jeres tid. Det er helt sikkert noget vi kan bruge til noget
197	P2	Velbekomme
198	P1	Det håber vi da.

Fokusgruppe 2 F

Linje nr.	Navn	Udsagn
1	M1	Ja, hvis vi lige kan få en kort præsentationsrunde, med navn, hvad i laver i COWi og hvor længe i har været her
2	P8	P8, vejingeniør ja, sådan primært projektering og jeg har været her i 6 år efterhånden
3	M1	ja
4	P7	P7 jeg har arbejdet med havneprojekter og har snart været her i 4 år
5	M1	
6	P6	P6, jeg sidder oppe i vejgruppen og laver vejprojekter, jeg kører noget projektledelse og BIM implementering og jeg har været her i hvad 10 år, ja
7	P5	Ikke mere?
8	P6	nej
9	P5	P5 og jeg er tekniskt assistent og jeg sidder i Geo-teknik gruppen og jeg har vel kun været her i 32 tror jeg det er blevet til
10	M1	I forhold til IT-sikkerhed hvor meget synes i det fylder i hverdagen her ved COWI? både handlingsmæssigt og tankemæssigt
11	P8	Jamen man kan godt mærke det er mere og mere. Altså vores frihedsgrad er indskrænket væsentligt på de 6 år, jeg vil faktisk sige på 2 år. Fra vi selv havde kontrol med vores pc'ere så er de jo gradvist ved at lukke ned for det, og det er nået dertil hvor de har lukket det så meget ned at vi ikke engang har adgang til de programmer som COWI faktisk bruger, så nu begynder det at blive så stort et problem at vi ikke kan producere i det samme omfang fordi vi skal igennem servicedesk og diverse bureaukratiske ting for at få lov at hente de mest basale programmer
12	M1	Så der er meget spildtid?
13	P8	Der kommer mere og mere spildtid, og jeg tror kun vi har set toppen af isbjerget indenfor det her og generelt inden for COWIs IT-systemer
14	P6	Ja vi er jo nået til et punkt nu også hvor det er et problem når du skal skifte pc så nu står du lidt i den situation at du har mere eller mindre ikke lyst til at skifte pc fordi der er for meget bøvl med at få skiftet, det tager halvanden uge inden den er oppe at køre, på grund af..
15	P8	I hvert fald hvis du har mange, altså basalt set jamen langt de fleste har adgang til de programmer de skal bruge, men ligeså snart du skal bruge et specialprogram der kører på licens jamen så kan du ikke bare have frit download. Og jeg forstår da godt at de lukker lidt ned for det så vi ikke helt selv kan styre hvad vi downloader, men det kan også blive for meget

16	P7	Det jeg har problemer med det f.eks hvis jeg skal have matcat f. eks. og så skal jeg ind og have nogle beregningsdokumenter så går jeg ind og finder der vi har alle beregningsdokumenter, og så skal jeg åbne den så man kan bruge eller bare KS eller check et eller andet. For at downloade det skal jeg først sende den der ansøgning for hvorfor jeg vil downloade nu, og så går der 24 timer, hvis ikke skal jeg ringe til service desk. så pointen er jo at når jeg skal KS det, så skal jeg forberede mig 24 timer inden fordi jeg kan jo ikke bare KS en halv time, for jeg har ikke programmet, ikke før i morgen. Men du kan f¨det, men s¨å skal du ringe til servicedesk og spørge om de kan lave en undvigelse, lige det her program kan de give mig, men så skal du også have en god grund. Det er det eneste jeg synes er lidt træls at hvis du kun skal åbne nogle, få lavet en KS eller bruge, altså noget du skal have nu, så kan du ikke, så skal du i hvert fald bruge 15-20 minutter for at få dem til godkende og så tager det alligevel lang tid og det er jo fjollet
17	P8	Og så i mellemtiden så kan vi i projektledelse prøve at oprette dig i cockpit
18	P7	ja, haha. den er lidt spøjs
19	M1	Er det fordi der er for meget sikkerhed eller er det forkert sikkerhed. Altså er det de rigtige steder de bruger deres energi
20	P7	Jeg ved ikke helt hvorfor den gør vi ikke kan downloade matcat for eksempel eller reyavik, jeg ved ikke helt hvor nogle vi ikke kan downloade
21	P8	Jeg tror de skal være lige lidt bedre til at se hvad for nogle. Så må de jo lave nogle undersøgelser og se hvad for nogle programmer bruger vi egentlig. Jeg kan forstå hvis der kun er en bruger i hele Cowi der bruger et special program. Matcat, autoturner og sådan noget, det bliver jo brugt i massevis hvorfor at de skal igennem det her. De skal bare være forhåndsgodkendt. Spotify det kan man så sige det er et program udefra, men hvis vi ikke stoler på spotify så kan så skal vi da ikke stole på noget mere. Det må vi selvfølgelig gerne downloade. Find ud af altså, lav en eller anden database over hvilke programmer der bliver brugt og så giv adgang til de programmer og så må de jo lave nogle stikprøverkontroller og se om de programmer, for jeg kan da godt forstå det fordi det man godt jo flere programmer man henter ind jo flere sårbarheder er der og det er jo ikke i forhold til mails, men i forhold til decideret hacker angreb
22	P6	Ja, men så du jo den der mulighed med når du installere fra nettet at du får den der fine boks op hvor du kan skrive. Du skal skrive et eller andet, men det er ligegyldigt hvad du skriver
23	P7	Ja, det er det også. Jeg tror det var computeren selv der ville opdatere og så kom den, hvorfor har du lyst til at opdatere og så skrev jeg bare fordi jeg sjældent gør det. Jeg havde ikke downloade noget program og så ville den opdatere og så skulle jeg skrive hvorfor jeg ville opdatere. Jeg havde da ikke bedt den om at opdatere det. Det var fint som det var
24	P6	ja DET ER JO SÅDAN NOGET DER IKKE rigtig GIVER mening når man har en boks der der kommer op for det første når du ikke selv har valgt det og for det næste at du kan skrive hvad som helst og der er ikke nogen der tjekker det i den anden ende, så giver det ikke nogen mening. Jeg tror ikke jeg har skrevet noget fornuftigt det sidste halve til hele år og der er ikke nogen der har spurgt om noget
25	P5	De har ikke forstået hvad der stod

26	P6	Nej, åbenbart ikke, men der skal jo bare stå et eller andet
27	P5	Så giver det ikke nogen mening at sætte den boks op
28	M1	Hvis vi lige går ind på der her e-kurser som vi lige har taget. HVad tænker i om dem, altså sådan den måde at få sikkerhedsinformation. Er det succesfuldt eller er der en bedre metode
29	P8	Nej jeg synes egentlig metoden er ganske fin. Der er lidt af hvert. Der er både en animation, lidt tekst hvor man også lige får lov at læse og så er der lige stikprøven til sidst som sikre man har læst teksten. Det synes jeg egentlig er fint. At der så er nogle elementer i det som måske er lidt kavt at man misforstår spørgsmålene så man svarer forkert, også selvom man læser spørgsmålet igen så tænker man det er jo en fejl. Så gider man ikke svare. Og jeg må først komme videre når jeg egentlig har svaret forkert. Men det kan også være vi tolker det forkert, men bare det at vi kan tolke det forkert jamen så er det jo ikke en ordentlig test.
30	M1	Så er det ikke formuleret rigtigt
31	P8	Og så var der sådan noget som, vi snakkede om de ikoner, som er, som overhovedet ikke giver mening, her klik på det her ikon, som ikke giver mening, jamen det mener jeg mere at det er sådan en stikprøve, for om man egentlig hopper i testen egen problemstilling, fordi du skal klikke på noget, som du ikke ved hvad er, for at finde ud af hvad det så er. Det er jo lige præcis det mails går ud på
32	P6	ja
33	P8	Så det, for mig, dernæst så kom der jo så en hvor der så var et intromærke ud fra til, fra, bcc…
34	P7	Det var bedre
35	P6	Ja det giver...
36	P8	Det giver mening, for så får man af vide, hvad fanden er det jeg gerne vil, ja hvad kan jeg forvente at undersøge frem for en eller anden, en mask og et uendelighedstegn, eller et eller andet, Så kan man først sidde og gætte på hvad det er
37	P6	Ja
38	P8	Der burde komme en eller anden op ‘’du røg i fælden’’, når jeg prøver den næste ‘’du røg i fælden’’
39	P5	Den har jeg ikke lige tænkt på
40	M1	Ja, så i syntes godt om konceptet, men indholdet kunne godt justeres lidt? er det sådan jeg skal forstå det?
41	P6	Ja
42	P7	Det er lidt for varierende
43	M1	Ja
44	P8	Ideen bag er jo rigtig fin
45	P6	Ja for som vi også snakkede om før, ja eller tidligere Hans Jørgen, det der med jamen altså, ved at ligge det derind og tvinge folk til at gå igennem det, så sikre man sig også at folk de om ikke andet læser bare lidt af det ikke
46	P7	Ja, men jeg tror også der er mange der bare skim læser det, bare læser hurtigt igennem, og så er spørgsmålet skal du åbne en virus mail, ja eller nej? øøh nej, altså
47	P6	Ja
48	P7	Men der har de ihverfald været igennem det

49	P5	Så kan man da sige at de har taget den til sig om ikke andet
50	P8	Men man skal aldrig lave en test, hvor man skal svare sandt eller falsk, og så at det er, at det ikke er entydigt, hvad man egentlig skal svare, og så når der så er svar, så kommer der…
51	P7	Du er stadigvæk sur over den der
52	P8	Jamen det er fordi, for sådan nogle tests der, når jeg tager sådan nogle tests der, så irriterer det mig faktisk at der så bagefter står, du havde forkert, selvom man nok godt kunne afslutte den lidt andet. Så tog jeg den sku lige igen, for jeg gad ikke at lukke sådan. Jeg ved ikke hvor meget COWI holder øje med os, så jeg ved ikke om der så popper op og siger, nu har du trykket forkert tre gange, om det så går ud i systemet at shit det der det er det svageste led i mails (kan ikke høre resten, 10:09)
53	P6	Ja så hun får ikke lov til at have mail
54	P8	Ja, men jeg kan bare ikke lide tests, hvor man egentlig får at vide at man svarer forkert, selvom man egentlig svarer rigtig
55	M1	Ja
56	P8	Det er bare, det går mig på
57	P6	Du svarer nok forkert, det er bare spørgsmålet der så måske er stillet lidt sjovt
58	P8	Spørgsmålet det er stillet sjovt, og det svarer den jo først, dengang vi så svarer rigtigt så forklarer den så hvad de egentlig mener
59	M1	Ja, tror i at hvis ikke de her ekurser var her, tror i så der ville være flere brud på sikkerheden? altså
60	P7	Jamen jeg tænker lidt at det der e kursus, det er en erstatning for at vi alle sammen skal sættes ind i kantinen og sidde og høre på nogen snakke om sikkerhed i en halv time, hvor tyve procent følger med, og når vi så bliver kastet ind i kantinen lige tirsdag kl ti, så er det ikke sikkert det passer for alle sammen
61	M1	nej
62	P7	Så på den måde så syntes jeg, at det, altså det er måske ikke verdenens bedste metode for at få folk til at lære det, men lige pt. så syntes jeg at det er den bedste alternative, fordi jeg ved at der er mange af mine medarbejdere som er projektledere som kan overskue det, når det er at du selv kan vælge at tage de sidste fem minutter på arbejdet, frem for at sige, lige tirsdag kl ti, der skal alle sammen sidde i kantinen og høre på at han snakker om noget, og få en quiz bagefter, eller hvad søren, vi tager det i plenum, altså så kan man jo sidde og diskutere, og så kan du jo bruge din aggression på samme tid(peger på P8), det er en fordel ved det, men jeg tror at mange får meget mere ud af det og selv kunne vælge det nu når det er online, og så er der nogen der vil bruge en halv time på det fordi de syntes det er meget interessant og læse og tage testen ti gange så må man gerne det, og hvis der er nogen der bare skimlæser igennem, og bare svarer det der er logisk i testen altså…
63	P5	Jamen så har de også forstået det stadigvæk
64	P7	Ja, så har de jo gået igennem
65	P5	Værre er det jo ikke
66	P7	Jeg tror det er det bedste alternativ der findes nu

67	P6	Ja men jeg tror, jeg ved ikke om den, altså, om den gør at det er mere sikkert, altså det er jeg sådan lidt i tvivl om. Der er nok nogen der lærer rigtig meget af det der, men jeg synes ikke umiddelbart der var noget i det der, der var overraskende, altså det er jo rigtig nok i beskrivelserne men man får jo ikke...
68	P8	Man bliver jo introduceret til de forskellige områder af mails, og det er jo fint
69	P6	Ja ja, men igen om det hedder en phisning mail eller malware eller falsemail eller hvad fanden det nu hedder
70	M1	Så det giver måske mest bare sådan lidt, at det sidder i baghovedet at man skal være skeptisk overfor mails?
71	P6	Ja
72	P7	Ja
73	M1	End at det som sådan er at man konkret ved lige de forskellige...
74	P6	Ja og så tror det er lige så meget også er spørgsmålet om, atlså en reminder om det
75	P7	Ja det tror jeg også, jeg tror ikke at det giver det store, men jeg tror også at det er træls hvis man ikke har lært det, altså fordi man begynder lidt at tænke på det
76	M1	Ja, så det får nogle tanker igang?
77	P6	Ja
78	P7	Ja en lille reminder, altså det er ikke fordi man pludselig bliver mega optaget af det, mega smart eller siger man har fået en helt n kompleks (13:10) men jeg tror, altså jeg tror ikke det giver nogle ulemper
79	M1	Nej
80	P7	Og den tager ikke så meget ekstra tid, man kan selv vælge hvornår man vil tage den. Jeg syntes det er godt nok den er der
81	M1	Ja
82	P5	Det kunne da være man lige lod være med at klikke bare i vildskab
83	P6	Men næste gang, så skal det være det der med ikonerne. Mærkelige ikoner man skal trykke på, så får man bare en over nakken
84	P8	Det er sådan de bør gøre det, det er at sende en mail ud til alle i COWI, og så skal de se hvor mange det er der trykker på den
85	P6	Ja
86	P7	Det kunne være smart, så fyrer man alle der trykker på den
87	P5	Så kommer der sådan en sort skærm, eller sådan et eller andet
88	P7	You got hacked
89	M1	I kom lidt ind på det tidligere at når man skal downloade noget, så skal man til at forklare det og sådan noget, men sådan generelt, syntes i der virker til at være tillid nok fra ledelsen til, altså til at i har, til jeres ansvar for it-sikkerhed, i syntes i at de er lidt for emsige eller hvad man skal sige
90	P6	Jeg syntes, altså ledelsen ved jeg ikke helt lige, men altså det virker som om engang imellem at COWI it (14:20) indfører noget for at holde sig beskæftiget, altså
91	M1	Ja, for at gøre det fordi det ikke rigtig hjælper (14:26)

92	P6	Ja, sådan set. Altså sådan noget som at fjerne administratorrettighederne på pcen så vi ikke kan afinstallere noget som helst, i min verden giver det overhovedet ikke mening. Altså at skulle ringe til servicesdisken for at få dem til at afinstallere et program for mig, altså, det giver jo ingen mening overhovedet
93	P7	Nej
94	P6	Ja og så ja virker det for mig som om at det er for at holde dem beskæftiget
95	P8	Men omvendt synes jeg også at det er en sikkerhedsforanstaltning de lidt er nødt til altså, det kan gøres på mange forskellige måder, jeg tror bare, jeg ved ikke om altså, de tager måske nogen gange bare et skridt lidt ekstra end at de lige selv kan følge med. F.eks. syntes jeg at det er rigtigt fint at der er sådan en, hvad hedder den, sådan en tovejs eller totrins godkendelse når vi åbner op derhjemme, men dengang de lige havde implementeret det og så et halvt år derefter så skulle man godkende med en sms op til 10 gange bare for at få lov til at starte sin computer op.
96	P7	Ja
97	P5	Der er lige lidt der
98	P8	Men det er jo et skridt de nok er nødt til at tage, men hvonår skal man implmentere det? Skal man teste det inden eller skal man bare hovedløs implementere det? Både den dialogboks der og så den med koden. Dialogboksen er i og for sig fin nok, men vi kan egentlig ikke se formålet i den så bliver den bare mere til irritation
99	P6	Ja
100	P8	Og det der med de koder, jamen når det bare er den ene eller to gange, så synes jeg faktisk det er rigtig rigtig dejlig. Bare sådan en sikkerhed for os hvis man skulle tabe, miste sin computer og der er en eller anden der bare lige, du kan sgu ikke logge på min computer.
101	M1	Det giver også en slags ro
102	P7	Bare gør det per 20 in logning eller per 30, bare ikke hver gang
103	P8	Jeg synes det fungere nu. Jeg kan godt leve med det
104	P7	jeg skulle først tage en sms for at komme ind på computeren eller ind på nettet og så ind på skype og så 4 sms'er, en for mail, en for skype og så sad jeg der og jeg skulle bare ind og skrive at jeg tager kage med fordi jeg har fået baby (16:30). Så jeg endte faktisk op med bare at sende en sms til Lasse og sige at du kan skrive en mail for jeg gider ikke.
105	M1	Hvis vi lige går ind på deth er med emails igen er det noget i sådan føler i ksla være meget opmærksom på. Får i mange mails som i godt kan se der er malware eller phsishing mails?
106	P6	Nej
107	P5	Nej
108	P6	Nej, der er nogle få der kommer igennem, men det er ikke ret mange.
109	P7	Jeg har aldrig set nogen
110	M1	Ellers så spamfilteret fungere ret godt?
111	P6	Spamfilteret fungere faktisk rigtig fint
112	M1	Og det tager ikke for meget?
113	P6	Jo, det gør det. Det tager interten mails.
114	M1	Okay, det er lidt spøjst

115	P6	Jeg har lige, altså i mandags var jeg til noget VR præsentation i Lyngby og der havde jeg tilmedlt mig. Svaret kom fra en over i kommunikation. Den ednte i spam, det synes jeg er lidt uheldigt og når der bliver sendt mail ud om aktier for eksempel så ryger de også i spam. Så jeg synes det er lidt uheldigt når COWI's egen mails ryger ind i spam.
116	M1	Det kan jeg godt forstå- Det giver heller ikke så meget mening
117	P8	jeg synes heller ikke det har været så galt, men vi har også prøvet hvor det kommer fra kunder og sådan noget, selvom det er Aalborg kommune så de ryger derned og så ringer man til dem og siger vi skal snart have jeres svar "Men det har vi jo sendt for 5 dage siden, vi sender det lige igen" og så går de på ferie og så tænker man forhelvede det er stadig ikke kommet igennem og så kigger man efter ferien og så siger man nå nu har jeg så haft det i min indbakke i 3 uger, men der skal man jo så bare huske man lige skal tjekke det spam filter en gang imellem, men det er nok mere fordi jeg synes der ikke har ramt så meget derover i
118	P6	Nej, men jeg synes egentlig også at når mailsene kommer udefra så kan de jo ryge der i, men jeg synes det er lidt til grin når COWI's egen mails
119	P8	Ja ja det burde ikke kunne lade sig gøre
120	P6	Det burde ikke rigtig kunne lade sig gøre at mails der kommer fra @cowi.com ryger i.
121	P8	Der kommer nogen gange nogen intern ting, jeg tror projektwise eller et eller andet på et tidspunkt der hvor vi skulle tage en test eller skrive bestillinger (18.40). Det kom fra en eller anden ukendt person måske med cowi.com bagefter, men jeg klikkede sgu ikke lige på linket for jeg tænkte det der det virker lidt mystisk.
122	P6	Ja
123	M1	Er der nogen sådan initiativer i selv tager altså ITsikkerhedsmæssigt, noget i selv gør fodi i tænker det kunne være smart, som i iikke direkte har fået at vide i skalgøre? Eller, nej?
124	P6	Nej
125	P5	Det tror jeg ikke
126	M1	Nej, okay. Nu skal man jo tage de der 3 om året, men i har egentlig adgang til 25 COWi har købt 25 forskellige så i selv kan gå ind og tage nogle af de andre er det noget i nogensidne har gjort altså taget flere af de sikkerhedskurser end de tre årlige i skal tage?
127	P8	Jeg var ikke engang klar over at vi skulle tage 3
128	P6	Nej det var jeg heller ikke. Jeg var heller ikke klar over der kom 3 årligt
129	P7	Næ
130	P6	Nu var der jo kommet 3 her vi skulle tage
131	M1	Er det noget i tænker i kunne have fundet på hvis nu i var blevet informeret om det
132	P6	Nej det tror jeg faktisk ikke. Det tager jo tid hver gang
133	M1	Det gør det
134	P8	billablity vi skal fakturere alt vores tid. Hvis vi måtte skrive det på adminstrationen så kunne vi da godt tage 35 kurser og have alt tiden til det.
135	M1	Hvordan fungere det med de 3 tests i tager nu? Er det på jeres egen tid

136	P8	Det er helt sikkert interessetid
137	P6	Jeg kan godt lide der er kamera på
138	M1	Men det er ikke et problem med at man ligesom tidsmæssigt at man føler man skal bruge sin egen tid på det, man kan godt få ind under altså kurset
139	P8	Ja, det synes jeg nok
140	M1	Det burde da også være sådan. har i ellers nogle forbedringsforslag, det kunne være til kurset eller bare generelt til IT-sikkerhed.
141	P7	Kan du ikke tage den der (peger på P8)
142	P8	Den er nævnt. Nej, men altså igen, jeg synes hoved princippet i kursusmaterialet er rigtig fint fordi det er, det kommer ind over de der tre områder og så er det egentlig relativt hurtigt kort og kontant og man bliver itroduceret til det og det behøver sgu ikke uddannet mere i det end det der for det kan også blive for omstændigt synes jeg for så begynder det at blive træls i forhold til arbejdstider og faktuerringer hvis det begynder at blive et halv times kursus
143	M1	Så er det heller ikke sikkert man er lige så koncentreret det sidste stykke tid
144	P5	Der er ikke nok der gider åbne for man tænker okay det tager nok en halv time det gider jeg simpelhent ikke.
145	P8	Bare allerede de her 10 minutters kurser, det ved jeg at, nu kom jeg jo tilbage fra barsel der så havde jeg jo fået masser af reminders på at jeg ksulle tage det. Der var rigtig mange af mine kolleger der kun havde taget det kursus fordi de var blevet trætte af de reminders.
146	M1	Får i noget at vide hvis nu i bliver ved med at få reminders uden at gøre noget ved det? Kan det så være jeres leder kommer og siger noget. Har i oplevet det?
147	P8	Nej
148	P6	Men jeg vil da gå ud fra at hvis der kommer ex antal reminders så kommer head of section og beder en om det vil jeg tro
149	P8	Det er vel også fint nok det er uddannelse ting vi alle sammen skal tage. remindersne synes jeg reelt set også er fine nok de er der fordi hvis det ikke var det så havde jeg glemt det.
150	P5	Så skete der ingenting. Så havde det kommet ned som nummer 90 mail. Så sker der ikke noget
151	P7	Så havde jeg aldrig fået dem lavet. De må gerne komme
152	P8	Så det synes jeg egentlig er fint nok for det er et kursus
153	M1	Ja, så er vi egetnlig mere eller mindre igennem det hele. Tusinde tak for hjælpen

Initierende interview med IT-ansvarlig hos COWI

G

M Vi vil gerne starte med at spørge lidt indtil COWI, og lige få dannet et overblik over COWI som virksomhed. Og senere gå lidt ned til noget IT-sikkerhedsmæssigt.

P Yes

M I forhold til COWI, hvordan vil du definere hvad COWI er?

P Altså COWI som forretning?

M Altså ja som virksomhed.

P COWI som virksomhed, er en stor international virksomhed som har omkring 7000 medarbejdere, hvor hovedparten er ingeniører, som man i relation til denne problemstilling skal tale ind til. Der er en meget høj grad af faglighed i den måde folk arbejder på. Ingeniør branchen er, hvis folk som jer andre ikke kender COWI, designer vi broer, tunneler, bygger veje, rådgiver, bygherrer omkring byggeri i forskellige afarter, så har vi sådan set en meget bred pallette af rådgivning omkring infrastruktur i dag. Vi er Danmarks andenstørste rådgivnings/ingeniørfirma, og det største det er Rambøll. Vi er fordelt globalt set, hvor hovedparten af vores forretning ligger i Skandinavien, hvor vi sådan ca. er 2000 medarbejdere i Danmark, 1500 i Sverige og 1500 i Norge og så er resten sådan runde tals bredt rundt omkring på jordkloden. Både i Afrika, USA, Canada, mellemøsten i øvrigt Asien, så vi er spredt godt og grundigt rundt over det hele.

M Ja, du fik enlig svaret på en del af mine underspørgsmål der, så det er perfekt. Hvis man sådan kigger på medarbejderen, kan man så sige at det er en fast rutine de kører hver dag, eller er det meget varieret sådan i deres arbejdsgang?

P Du kan jo sige det er det samme de laver, også er det jo alligevel ikke. Vi lever af at være innovative, vi skal hele tiden forsøge at gøre vores ydelse bedre, billigere og anderledes end hvad vi gjorde i går. Så selvfølgelig er der et element af at bruge den viden, man har oparbejdet fra tidligere, men der er også hvordan vi gør den viden mere tilgængelig så vi kan levere ydelsen billigere. Så det er bestemt ikke rutine arbejde, det er ydelses arbejde det vi har med at gøre.

M Kan du kommet lidt mere ind på din rolle hos COWI?

P Det kan jeg i hvert fald. Jeg er det man kalder IT-sikkerhedschef. Det vil sige at jeg har det overordnede ansvar for at sikre at det man med et flot ord kalder GFC, government risk and compliance er på plads. Det vil sige at jeg skal orkestrerer at vi har de tekniske og organisatoriske sikkerhedsforanstaltninger, til at beskytte det vi nu skal beskytte. Og det er en del fortrolighed vi ønsker at beskytte her i gesjæften. Men det er måske i lige så høj grad tilgængelighed af information. Vi sælger timer, COWI lever af at sælge timer, så ethvert led brud på systemer eller andet der gør vores folk uproduktive, og det koster penge. Så det vil vi for alt i verden undgå. Og det er så min opgave at sikre at IT indbygger de mekanismer de skal, for at holde vores grej i luften.

M Er det så i forhold til de danske ansatte, eller er det også COWI international set?

P Ja, det er COWI group. Så det er internationalt set.

M I forhold til COWIs ledelsesstruktur, kan man så sige at i har en flad ledelsesstruktur eller er den mere hierarkisk?

P Den er meget hierarkisk, og meget decentraliseret. Sådan er naturen i ingeniørbranchen i og med at det er højtuddannet arbejdskraft man benytter sig af, er der en meget høj grad af selvstændighed ude omkring. Det er nok svært at være topleder i en virksomhed som denne her, bare fordi topledelsen siger noget, behøver det ikke at betyde at sidste led i et projektkontor i Ghana opfører sig som topledelsen nu synes. Så man er meget individuel her i firmaet.

M Okay, så går vi lidt mere over til IT-sikkerheden. Hvor vigtig er IT-sikkerheden hos COWI, hvor højt er den prioriteret?

P Det kommer jo så an på hvem man spørger, der er jo efterhånden, hvis du læser COWIs årsrapport, den er jo offentlig tilgængelig. Den kan du læse fra sidste år, her vil du finde ud af med de briller på at der står ikke ret meget om IT-sikkerhed, eller IT risk, eller teknologi risk i den årsrapport. Men der er jo ingen i COWI i dag der kan levere noget som helst uden IT, alt er jo IT båret. Samtidig med det er vi jo også i en periode hvor alle råber på digitalisering, vi skal digitalisere det ene og det andet og det tredje. Så der er jo en gryn af forståelse af, at det kan vi ikke gøre uden at tænke sikkerhed væsentlig mere end hvad man har gjort historisk set. Historisk set kan man sige at ingeniørerne været, nu skal jeg passe på at sige noget der ikke lyder forkert, men det er ingeniørerne der har haft bukserne på. Det er dem der har bestemt præcist hvordan de skulle arbejde, med hvilke værktøjer de skulle arbejde og det har de

fået lov til. Fordi op igennem historien har man nok tænkt mere innovation og produktivitet end man har tænkt sikkerhed. Men det er helt klart et billede som stille og roligt begynder at ændre sig nu. Der er jeg jo frygteligt godt hjulpet af andre kollegaer i branchen, som har været ramt hårdere end COWI har været ramt. Det startede jo for et par år siden med mærsk nedbruddet og her i sidste måned har vi haft demant nedbruddet og det er altså noget som ledelse og bestyrelse kan forstå, at hvis man går så meget på røven som de to virksomheder har gået, koster det altså mange penge. Og det vil det jo også gøre i et COWI regi, hvis vi bliver lagt ned af noget, som lægger os ned i 2-3-4 uger, er det så markant en risiko, at det er bestyrelsen der er begyndt at bekymre sig rigtig meget om det.

M Som du siger i takt med digitalisering, er der så også kommet et større IT budget hos COWI i nyere tid?

P Ja det er der, vi benchmarker vores COWIS IT investeringer, i forhold til, jeg ved ikke om i kender til det her analyseinstitut, der hedder Gartner.Det er et stort it analyseinstitut, som sådan nogen som mig hører meget godt efter, de benchmarker hver andet år, eller de gør det faktisk hvert år, hvor meget it man spenderer i forhold til sin branche, og i øvrigt sin omsætning, og der har cowi over de sidste, lad os sige 8 år, brugt kontinuerligt mere på it end vores kollegaer i branchen

M Okay, ja det er da et godt svar. Ja, kan du fortælle noget om en følsomme data i har behov for at beskytte?

P Ja, de kommer i to kategorier. De data vi producerer, de er som regel ikke følsomme som sådan. Ofte ejer COWI ikke de data vi producerer, vi producerer for nogen. Så det er ikke hemmelige data som sådan, når vi snakker tilsyn og når vi snakker tegninger, den slags. Så for vores primære virke, der er byggerier, broer og tunneler og så videre, der er vi kun bekymret om tilgængeligheden af information, vi er ikke bekymret for fortroligheden. Så har en anden forretning, hvor vi rent faktisk dataanalysere for forskellige kunder. Her er vi faktisk ofte databehandler af både følsomme og normale persondata. Det kan eksempelvis være at en kommune gerne vil have belyst uheldsstatistik i et farligt vejkryds, kombineret med årsagen, altså om der har været alkohol indblandet, eller fart eller noget andet. Den slags dataanalyse er også noget vi laver, hvor vi kombinerer vores viden omkring kort og infrastruktur, med datakilder fra forskellige steder i kommunen. De skal selvfølgelige beskyttes på et andet niveau. Og så har vi lige den sidste krølle på det, og det er når vi er ude at rådgive forsvaret, eller svenske og norske atomkraftværker. Det er en type data som bliver kørt helt uden om COWI som sådan. De bliver kørt i det der hedder dark sides, altså i fuldstændig isoleret infrastruktur komponenter, så det

beskytter vi helt ekstraordinært, men det er så også et krav for kunden, hvordan og hvorledes.

M Ja okay. Er i stødt på nogle udfordringer i forhold til COWIs ansatte, at der er nogen grupper der er mere udsatte for at kunne lave de her human errors end andre?

P Jamen når du snakker human errors, så kunne jeg godt forledes til at tro, at det er og lave en forkert beregning på en bro så den falder ned. Men det tænker jeg ikke, at det er det du spørger efter?

M Nej jeg tænker mere i forhold til et it brist, altså sikkerhedsbrist, på den måde ja

P Der vil jeg sige nej, der er nogen roller der naturligt er, er mere følsomme og interessante for de cyberkriminelle, men alle vores medarbejdere kan dybest set blive phishet, eller på anden måde kunne starte et cyberangreb. Så på den måde har jeg en meget sådan homogen medarbejdergruppe, jeg har jo ikke sådan white collar workers og blue collar workers hvor jeg skal differentiere væsentligt i den undervisning de skal have. Jeg kan målrette den en lille smule til de forskellige, men de er grundlæggende alle sammen white collar workers, altså kontornussere hele bundet.

M Ja, så det er meget det samme. Og i forhold til det danske og det internationale, der er heller ikke nogen forskel?

P Der er så til gengæld sjovt nok markant forskel. I danmark, norge og sverige, bare for at tage den, der er markant forskel på måden man tænker sikkerhed, på måden man agere. COWI i Norge er langt mere modent på det område, der har man gennem væsentligt flere år tænkt sikkerhed, og sikkerhed er en del af dna'et i norge, væsentlig mere end at det er i sverige, så der er meget stor forskel på regionerne. Og så har vi jo noget som nordamerika, hvor der for alvor er en helt anden type lovgivning, der i virkeligheden trigger den den måde man tænker privacy og sikkerhed ind i det man arbejder. så der er meget store regionale forskelle

M Okay, og det bunder mest i kulturelle forskelle? er hvad vil du vurdere. Det er måske svært at sætte ord på hvad det helt præcis skyldes?

P Altså det skyldes jo en kombination af det marked man operere i, og den lovgivning man er underlagt i det marked. De to ting kommer jo til at præge din kultur meget. I Norge f.eks. har vi i mange år haft en stor business med olie og

olieboreplatforme og den slags, og det er virkelig sådan et sted hvor sikkerhed, og det er jo også fysisk sikkerhed, det spiller en væsentlig rolle, så hvis vi har en kunde, en stor olieboreplatform, så stiller de nogle krav til COWI personale og så bliver det en del af kulturen at tænke sikkerhed ind, langsomt men sikkert

M Ja okay. Det var sådan set lige det vi havde til it sikkerhed sådan lidt overordnet, så jeg vil godt gå lidt over i hvad COWI gør, sådan rent praktisk. Så hvad gør COWI lige nu for it-sikkerheden, for at informere om det?

P For at informere om det? for 3 år siden, der startede vi med et security awareness program. COWI vil gerne arbejde efter ISO-27000 standarden. Og i den er det sjovt nok dikteret, at man blandt andet skal informere sine medarbejdere om sikkerhed. Men, eftersom vi er så mange mennesker, og vi er spredt ud på så mange steder, så er det eneste rigtige og gøre, det er at køre noget e-learning ud til vores medarbejdere. Det gjorde vi for første gang, for 3 år siden. Der købte vi et e-learning program hos deloyt, der bestod af ti små moduler, hver af 4-6 minutters varighed, og dem skulle medarbejderne tage som obligatorisk træning. Og det blev der fulgt op på ugentligt, at de nu fik taget deres træning. Det gjorde vi for 3 år siden, så her i år, der har vi købt et nyt system, igen e-learning, men vi var ikke helt tilfredse med det træningsmodul vi havde købt fra deloyt, så vi købte et fra et canadisk firma, som vi har kørt ud nu de sidste par måneder. Og vi har købt 25 moduler, også af sådan der 5 minutters varighed og så gør vi så det at vi tager 3 aktuelle emner, altså 3 moduler og gør obligatoriske hvert år, ud af den her portfølje af 25 moduler. Så det er sådan det man kan kalde security awareness træning. Det er nok det jeg gør primært i udover at vi forsøger at holde oplysningskampagner på vores intranet, men der er vi lidt hæmmet af at vores intranet kun eller artikler på vores intranet bliver læst, lad os sige, mellem 2000 og 3000 gange. Det vil sige jeg når slet ikke ud til alle de medarbejdere jeg skal ud til via vores intranet.

M Ja og hvad er det helt præcist i søger at opnå med de IT-sikkerhedskurser. Er det ligesom at informere mod de trusler der er?

P Ja både og, men det er i høj grad awareness. Det er i høj grad at flytte det op top of mind. Phishing emails. Vi har allesammen modtaget dem. Vi har allesammen været tæt på at klikke på noget vi ikke skulle klikke på. Nogen af os har måske endda gjort det. Og det er vi altså nødt til informere om kontinuerligt sådan hele tiden så det nytter ikke hvis jeg har kørt en awareness kampagne på phishing for to år siden. Ved du hvad jeg har sgu nok skiftet et par tusinde medarbejdere og man kan sgu heller ikke rigtig huske hvad man lærte dengang. Så det er hele tiden i mindre portioner få det top of mind sådan at folk tænker over det. Folk bliver eksponeret for trusler mere eller mindre hele tiden uanset om det så er i privatsfæren eller på jobbet og det er i virkeligheden det jeg

ønsker at fremavle, det er at man er oppe på tæerne hele tiden. Jeg siger ikke og jeg slår ikke hårdt ned på hvis folk kommer til at kvaje sig og klikke på noget de ikke skulle have klikket på. Ved du hvad, det kan vi alle sammen komme til, men det er vigtigt at jeg i videst muligt omfang får informeret om best practices til medarbejderne.

M Ja, og føler du det er opnået, altså ligesom at folk er mere opmærksomme på det i dag?

P I dag er de mere opmærksomme på det. Klart, ja. Er det så fuldt min fortjeneste? Ej, ikke rigtig. Der er også sket noget i hele billedet. Det er væsentlig mere omtalt i pressen i dag omkring cybersikkerhed, omkring trusler end det var bare for tre år siden.

M Ja.

P Så der er jeg godt hjulpet, men der er i dag væsentlig større awareness i organisationen omkring det her område og jeg får i dag væsentlig flere spørgsmål fra folk og bekymringer fra folk om gør jeg nu det rigtige, hvad med denne her, hvordan skal mit password se ud og så videre end jeg gjorde for tre fire år siden.

M Ja, altså interne COWI ansatte?

P Fra interne COWI medarbejdere, ja.

M Okay. Du nævnte det var 3 om året man skulle igennem? Var det det du sagde?

P Ja. Det er sådan et tradeoff mellem hvor meget tid må jeg bruge på det her altså når det er 3x7-8 minutter, jamen det er 20 minutter gange 7000. Altså man kan hurtigt i sådan en butik som vores, jeg fortalte også at vi sælger timer, så alt hvad jeg kommer ud med skal jo omregnes til timer som medarbejderne ikke kan fakturere til kunderne. Det er sådan lidt tradeoff med hvor meget kan jeg bruge kontra hvor meget for vi ud af det.

M Ja, men det kan jeg egentlig godt forstå. Er det så et bestemt tidspunkt på året eller er det bare i løbet af et år de tre skal gennemføres.

P Det er en kampagne vi kører sådan at vi skyder tre ud og så har de en måned til lave dem

M Okay så man får en ad gangen kan man sige?

P Ja altså tre på en gang op så har de en måned til at gennemgå de tre moduler og så næste år så vil vi så evaluere, jamen skal det være 3 helt andre moduler eller skal vi fortsat have et phishing modul ind eller har risikobilledet, har trusselsbilledet ændret sig siden vi kørt den sidst

M Ja, så i har ligesom 25 videoer at vælge ud fra og så ud fra dem vælger i så hvad der er mest aktuelt

P ja og de 25 videoer er tilgængelige for vores medarbejdere. Der er ikke en kæft der tager dem, men de er sådan set tilgængelig for dem der rigtig rigtig gerne vil. Der kan de bare slå sig løs i vores learning-management system som vi kalder COWI academy

M Ja og er det alle medarbejdere der skal igennem de her IT-kurser?

P Ja. Som jeg siger, der har jeg så ikke helt fået min vilje, jeg siger alle der bliver udstyret med adgang til COWI, de skal igennem dem. For alle der har en COWI pc eller adgang til COWI er en trussel, så dem vil jeg have fingrene i, men af licens mæssige issues har man ikke ønsket at investere i så mange licenser til vores learning-management platform

M Okay.

P Så alle fastansatte medarbejdere, dem når jeg ud til. Jeg når ud til 7200 medarbejdere i dag, men sådan en som dig, eller den relation du har til COWI hvor du bliver hævet ind i et par timer her og der og noget tilkald, det er ofte jeg ser at det ikke berettiger til at du har et login og en adgang til systemet.

M Altså til COWI academy eller bare generelt til..

P Til COWI academy

M Ja okay, jeg tog de der test fra Deloitte dengang jeg arbejdede der.

P Nå okay, jamen så vil du også have, hvis du har den samme login i dag, så vil du også kunne se dem, men det er også hvis vi hyrer konsulenter. Konsulenter får et andet type login end du gør som medarbejder. Dem har man ikke ønsket at investere licenser i..

M Hvad med deltidsansatte? Hvad med dem?

P Deltidsansatte burde, hvis de har et normalt login, så burde de have adgang.

M Ja og kan du sige noget om hvad for nogle praksisser i ligesom forsøger at give medarbejderne sådan i forhold til at tjekke emails en ekstra gang og ikke gå ind på links på hjemmesider de ikke kender og så videre. Hvad for nogle praksisser kan man sige i ligesom prøver at få dem til at tænke over

P Jamen det er i virkeligheden langt hen ad vejen best practices vi prøver at prædike. Og hvad fanden er det så. Ja det er jo, best practices ændre sig jo over tid. For at give jer et eksempel vi står lige i øjeblikket, en af de moduler vi har kørt ud, det er omkring passwords - at hvordan lave rman et sikkert password, hvordan ændre man det. Skal man begynde at snakke passphrase og så videre og så videre. I de fleste virksomheder som det er i dag der er der krav om at password skal være 8 karaktere og det skal være komplekst og man skal skifte det hver tredje måned. Sådan er det også i COWI, men på det seneste der er den anbefaling faktisk ændret. De kloge hoveder har jo faktisk fundet ud af at det sådan set er mere sikkert at have et længere password og så til gengæld ikke skifte det så ofte, men lige nu er COWI og COWIs systemer ikke klar til at ændre på vores passwords praksis så vi underviser fortsat i at et password skal være komplekst og det skal være 8 karaktere og du skal have et unikt password til alle de forskellige tjenester du bruger, du skal ikke genbruge dit password og du skal have en password manager til at huske alle de mange passwords du nu får opbygget fordi du ikke må genbruge. Det er mange af de praksisser vi har undervist i her i password.

M ja

P Så har vi undervist i cloud-security. det er jo kommet ind med stormskridt. det her cloud noget. den menige medarbejder tænker sgu ikke over om man bruger en service der er stillet til rådighed af Group-IT, eller om man bruger en cloud tjeneste i Usa. Så der har vi sådan prøvet at undervise lidt i, jamen .... mange af de her cloud-services er jo fine og sikre nok, men så er der også bare nogle af dem du skal holde snitterne væk fra. så der er man nødt til og… Der er ikke sådan en one size fits all praksis, men der er nogle gode råd hvor den enkelte

medarbejder skal begynde at forholde sig til det data man arbejder med. Det her data man arbejder med, egner det sig til og udveksle i drop-box eller er det noget hemmeligstemplet som man skal holde inden for virksomhedens fire vægge, eller hvordan er det lige det er med det.

M ja okay, i forhold til det du sagde med at COWI ikke var klar til at ændre koder til den nye måde at gøre det på er det fordi at det er en stor overgang som kræver en del , eller hvad skyldes det at man ikke kan gå med til det.

P til dels skyldes det, det er lidt den dårlige undskyldning, dels skyldes det de tekniske systemer. Det er ikke alle vore systemer der kan det, men det tror jeg i virkeligheden er det mindste af det hele. Jeg tror den største opgave i at gå over til et nyt password system det er den der change management ude i virksomheden. Og igen er det jo lidt et trade-off. Du har et password. Vi kender det allesammen, vi laver et password og så skifter vi tallet efterfølgende hvert kvartal når vi bliver bedt om det. Og det har folk jo været vant til. Hvis jeg nu går ud og beder dem om at hver gang de kommer på arbejde skal de indtaste et password der er 18 karaktere langt, men tilgængeligt behæver de ikke skifte så tit, men de skal taste det ind hver dag. Der er noget bearbejdning af kulturen for at det vil komme til at ske. På et eller andet tidspunkt der er jeg overbevist om at vi nok skal nå derhen, men det er nok vi sådan tænker over hvordan vi får succesfuld lanceret.

M Ja det kan jeg godt se, der er en masse underligende ting man skal tage højde for.

M Ja, okay jamen det var det i forhold til jer og IT-sikkerhed, og går over til jeres oplevelser. Har i haft nogen sikkerhedsbrug som har været grundet menneskefejl?

P Ja, det har vi da. Nu kan jeg jo så tage et meget godt eksempel, også fordi der ikke skete noget. Vi har en medarbejder der bliver phishet og det sker der ike noget ved. det lægger medarbejderen ikke mærke til, andet end hun udleverede hendes brugernavn og password. Så får de kriminelle adgang til hendes mail. Det har de i en måneds tid. Den her medarbjeder sidder i vores bogholderi, så de kriminelle har fuld lejlighed til at sidde og følge med i fakturabehandling og hvordan ser den ud. Og de er så i stand til at forfalske en faktura på meget meget meget vellignende vis, ved at have adgang til hendes e-mail boks. Så de kan sådan set tage en fuldstændig legitim faktura og ændre kontonummer på den og forsøge at få den igennem systemet, og det lykkedes næsten. DEt blev

fanget i nogle af de kontroller vi i øvrigt har, men du kan stort set ikke se på denne faktura den er falsk, den er så vellavet at hvis vi havde sovet en smule i timen så havde vi været 150.000 $ fattigere. Så alle kan blive phishet og alle kan komme til at klikke på et eller andet i en travl hverdag i en situation som de ikke lige tænker over og de kriminelle er godt klar over i dag at de tekniske sikkerhedforanstaltninger er så stærke at det tager lang tid at bryde ind i dem, hvor det er langt nemmere at manPulere med mennesket og få dem til at gøre det hårde arbejde. Få dem til at levere deres password eller andet. Så jo vi har været ramt af angreb hvor man kan sige the human factor har været udløsende.

M Ja, du sagde denne fejl blev opfanget fordi i har nogle kontroller, kan du uddybe det lidt?

P Det er at der lige skal være et ekstra sæt øjne på en faktura, når betalingsandragelsen ændres. Hvis nu det havde været den samme medarbejder der kørte den igennem, så var den sgu ikke blevet opdaget, men vi har lige det her ekstra kontrolelement der hedder, skal der ændres en konto så er der et four eyes princPle, altså et ekstra set jne der lige ser om det kan være rigtigt. Og så opdager hende her der blev fishet og reagere “jamen det er sgu da ikke mig der har sendt den her til viderebehanling” og så fanger vi den. Så det er organisatorisk kontrol der lige fanger noget der kommet igennem de tekniske kontroller.

M Ja okay, har de her tilfælde i har haft, har det fært til nye implementeringer, hvor i har set at nogen af de ting der er sket, og hvordan i kan forbedre jer mod det.

P Nej. Jeg kan ikke sige at vi har haft en angreb eller andet hvor jeg har sagt at lige præcis denne here tekniske dims er eller hvad det nu kan være, er installere på baggrund af det angreb. Det er mere at vi de sidste 2 - 3 år i den grad har styrket sikkerheden all.over. Jeg har ikke en enkelt hændelse jeg kan sige det er på grund af det her, det er mere på grund af det øgede digitalisering og det øgede trusselsniveau der er mod firmaer.

M Så det er mere ydre påvirkninger, hvordan det hele bevæger sig, end det har været interne ting der har gjort det er som det er i dag.

P Ja, altså en kombination. Det er en erkendelse af at vi ikke har gjort det godt nok kombineret med trusselsniveauet mod danske virksomheder

M Tror du fremtidigt at COWI vi bruge endnu flere penge på IT-sikkerhed?

P Ja det ror jeg helt sikkert. Så længe der er et økonomisk insitament til at angribe virksomheder, bliver vi angribet, og det er ikke noget der går væk i morgen. Og jeg tror heller ikke IT i virksomhederne går væk i morgen. Så dermed har man også et regnestykke der er nemt at regne på. Ja så er man nok næd til at beskytte det med IT-sikkerhed going forward

M Er det noget du synes på nuværende tidspunkt skal bruges flere penge på eller synes du COWI er godt dækket ind

P I forhold til den branche COWI arbejder i, der er vi tilpas dækket ind nu. Det er jo også meget at gøre med compliance og hvad for en lovgivning du skal overholde, det er klart at et finansielt institut, en bank. Skal overholde væsentligt strengere regler end en privateget virksomhed som COWI skal. Grundlæggende skal vi ikke rigtig overholde nogle regler, andet end den grundlæggende lovgivning, gdpr og så en boføringslov, det er det mere regnskabstekniske. Men har jo som sådan ikke et rammeværk, som vi skal kunne demonstrere compliance til. Så det er jo klart vi kommer aldrig nogensinde til at bruge så mange penge på it-sikkerhed som en finansiel institution gør

M Nej, ja, og hvad kan man sige de primære trusler er, er det udenlandske trusler eller?

P Det ved jeg ikke, men primære trusler mod danske virksomheder, kan i læse i det danske cybersikkerhedstrusles billede, men mod os, vi er ikke i en branche hvor vi bliver målrettet angrebet. Det er langt overvejende oportunistiske angreb, der bunder i finansielle motiver, det er jo ransomware, det er sådan noget, det er det vi ser, så længe der er økonomi i det, så længe der er penge i det, så bliver man angrebet.

M Ja, okay, Kan du sige noget om hvordan ledelsen ser på problemet?

P På hvad for et problem tænker du på nu?

M Altså på it-mæssige trusler..

P Ja, altså det er jo dybest set ledelsen der tager beslutningen omkring hvordan de vil agere i trusselsbilledet. Hvad for nogle risici vil vi acceptere, hvilke risici vil vi ikke acceptere. og der fungere det typisk sådan at os hernede på gulvet, vi kan udarbejde det risikobillede, hvad er det for en risiko vi ser mod de it-tekniske systemer og det tegner jeg et pænt risikobillede op af og rapportere det til vores ledelse, med en anbefaling om at hvis i synes at den her specifikke risiko er for stor, så kan i nedbringe den ved at uddanne jeres medarbejdere, eller købe et nyt stykke hardware eller et eller andet. Så ledelsen ser jo udviklingen i det her risikobillede og navigere herefter.

M Ja, føler du den menige medarbejder deler det blik som ledelsen har, eller er der nogle spændinger der?

P Jeg tror den menige medarbejder har et mere realistisk forhold til sikkerhed, jeg tror ledelsen i COWI, som i så mange virksomheder, de vil sgu godt have det her til at gå væk, de et eller andet sted, jeg vil ikke sige lukker øjnene for det, men det er noget at, en ting gælder for virksomheden og en anden gælder for direktøren

M Ja, ser du nogle problemer i de forskellige opfattelser, eller fungere det fint?

P Dybest set så er der jo altid den problemstilling, hvad sker der hvis chefen gør noget andet end der står i politikken eller hvad håndbogen nu er, dybest set så underminere det jo, det der foregår i resten af butikken, altså walk the talk. Så man gør som ledelsen, det er klart at hvis ledelsen ikke gør det de skal, eller noget helt anderledes, som ikke at sætte password på deres telefon eller hvad fanden ved jeg, så føler resten af virksomheden , så kan man jo bare gøre det for det gør direktøren jo

M Ja, så det forbillede er også en meget stor del af det kan man sige?

P Indiskutabelt, ja

M Nu er vi sådan set igennem alle de spørgsmål som vi havde forberedt, vi har lige lavet et lille bonusspørgsmål om der var noget som du tænker kunne være relevant. for os at vide som vi ikke har været inde på endnu

P Ja men ja

M Det er også svært at svare på

P Nu skal jeg lige tænkte tilbage på hvad det er i har spurgt mig om, altså hvad er det sådan, udover det mennesklige element i cybersikkerhed som i skriver om..

M Det er meget sådan med fokus på kommunikationen, som vi så gerne vil analysere

P Ja

M Det kan vi også lige snakke om, det der med de e-learning, det lød ikke til at det var så nemt for os at få adgang til

P ja,jo hvis du har haft adgang til det, til det gamle fra DELOITTE de lå i COWI academy, så burde du også have adgang til dem her, altså hvis du har et login hos jette, har du stadig en computer eller hvordan eller hvorledes? Det er en spørgsmål om at du laver en aftale med Jette. Der er ikke på den måde noget hemmeligt i det, det er bare praktikaliteten

M Okay, hvad må vi så med det? Må vi teste det, tage screehshot, eller er der rettigheder på det?

P Der er rettigheder på det, men i må gerne tage screenshot af det. I må bare ikke kopiere indholdet og der er iøvrigt også cowificeret, så der står COWI på det, men det er selvfølgelig licensbaseret

M OKay, jamen jeg tror ikke jeg kan finde på mere, jeg prøver at tage kontakt til jette så eller en anden i Aalborg afdelingen og høre mere om det. Vi snakkede lidt om at lave noget fokusgruppeinterview og spørge ind til testene.

P Det er fint, det er fint, skal jeg gøre noget andet?

M Det tror jeg ikke, jeg ved ikke om der kunne noget, om jeg så kunne sende en mail til dig, ellers kan jeg ikke lige se hvad det skulle være.

P Ja, ellers må du jo bare vende tilbage.

M Ja, men ellers så tusind tak for hjælpen, det har været nogle gode svar, der er en masse vi helt sikkert kan bruge.

P Held og lykke med det, godt, hej

M hejhej

Samtykkeerklæring H

Samtykkeerklæring til brug af audio/videooptagelser

I forbindelse med studerende _____ og dennes projekt på 3. semester omhandlende COWI's kommunikation af IT-sikkerhed, giver jeg hermed min tilladelse, til at sessioner må bruges som en del af den studerendes uddannelse ud fra følgende aftaler og specificeringer:

Jeg giver min tilladelse til,	JA	NEJ
- at sessionerne må videooptages	☐	☐
- at sessionerne må audiooptages	☐	☐
- at udvalgte klip af materialet må forevises projektvejleder og eksamenscensor	☐	☐
- at skriftlig beskrivelse og analyse af materialet i anonymiseret form må bruges i forbindelse med den studerendes 3. semester projektrapport.	☐	☐

Forudsætningen for denne samtykkeerklæring er, at alt materiale bliver opbevaret sikkert og fortroligt i henhold til Datatilsynets kravs. Materialet bliver opbevaret indtil endt eksamen i Januar 2020, hvorefter det slettes. Alle der har tilladelse til at se materialet har tavshedspligt. Det er altid muligt at trække denne samtykkeerklæring tilbage, hvorefter video- eller audiomateriale vil blive slettet.

_____ _____

Deltagers navn Studerendes navn

_____ _____

Dato Deltagers Underskrift

Spørgsmål angående samtykke er velkomne, og du kan kontakte den studerende på følgende e-mail:

_____

Godkendelse af litteratur I

RE: HASTER-HASTER Godkendelse af litteratur fra gruppe 3

Pirkko Liisa Raudaskoski

to 19-12-2019 08:34

Til:Lasse Jakobsen <ljako13@student.aau.dk>;

jeg godkender litteraturlisten

From: Lasse Jakobsen
Sent: 18 December 2019 20:56
To: Pirkko Liisa Raudaskoski <pirkko@hum.aau.dk>
Subject: HASTER-HASTER Godkendelse af litteratur fra gruppe 3

Hej Pirkko

Vi har lige fået en mareridts besked om at vi skal have godkendt vores litteratur inden vi kan aflevere projektet. Er dette noget du har hørt noget om?

Vedhæftet finder du vores litteratur. Håber du kan godkende.

Hilsen Lasse // Gruppe 3

Figur I.1. Godkendelse af litteratur