Emilie Forbord Dalen

Digital læring og informajonssikkerhet

Bacheloroppgave i Digital forretningsutvikling
Veileder: Kirsti Berntsen
Mai 2019

Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for datateknologi og informatikk

NTNU
Kunnskap for en bedre verden

Bacheloroppgave 2019
Studium: Digital Forretningsutvikling

Tittel - norsk: Digital læring og infrmajonssikkerhet *Tittel - engelsk:Digital learning and Information Security*		*Oppgave nr.:50D*
Oppgavestiller: NTNU		
	Kontaktperson: Emilie Forbord Dalen	
	Telefon:48222094	*E-postadresse:emiliefd@stud.ntnu.on*
	Postadresse:	
Studenter: Emilie Forbord Dalen		
Veileder ved NTNU: Kirsti Berntsen		

Sammendrag: E-læring er i dag et utbredt verktøy innen arbeidslivet, og tilrettelegger for fleksibel kompetansebygging og opplæring av både ansatte og ledere. E-læring bidrar til at læring kan foregå hvor som helst, når som helst. Flere eksterne aktører utvikler i dag e-læringspakker for sikkerhetsopplæring til de ansatte. Ansattes kunnskap og bevissthet om informasjonssikkerhet er en viktig forutsetning for å kunne ivareta informasjonssikkerhet. Ettersom informasjonssikkerhet ikke bare krever en økt bevissthet, men også en endring i de ansattes holdninger og atferd vil denne studien undersøke om det er noen aspekter ved digital læring som kan påvirke ansattes holdninger og atferd i forhold til sikkerhet.

Abstract in English: E-learning is a widespread tool in the workplace, and facilitates flexible competence building and training of both employees and managers. Through e-learning, learning can take place anywhere and anytime. Several businesses are currently developing e-learning packages for security training and awareness. Employee knowledge and awareness of cybersecurity is an important prerequisite for being able to safeguard information security. As information security not only requires increased awareness, but also a change in employee attitudes and behaviors, this study will investigate whether there are any aspects of digital learning that can affect employee attitudes, knowledge and behavior regarding information security.

Marker med kryss det som gjelder denne oppgaven:	
X	*Normalsituasjonen: Studentene har selv alle rettigheter knyttet til resultatet fra bacheloroppgaven, med de unntak som er beskrevet over.*
	Oppdragsgiveren har rettighetene og kan utnytte produktet kommersielt og videreutvikle produktet/metoden. Instituttet vil ikke utnytte produktet kommersielt, men vil kunne arbeide videre med den grunnlagskompetansen som er vunnet gjennom prosjektet, som beskrevet over.
	Resultatene fra arbeidet legges ut som OpenSource iht lisens *_____ (Se http://creativecommons.no/lisenser.*
	Bacheloroppgaven (det skriftlige arbeidet) skal være undergitt utsatt offentliggjøring i ____ (maks 3) år.

Forord

Denne bacheloroppgaven er skrevet ved Institutt for Datateknologi og Informatikk hos NTNU. Oppgaven er avsluttende del i bachelorstudiet Digital Forretningsutvikling, og ble skrevet våren 2019.

Jeg har lært mye underveis i skriveprosessen som jeg vil ta med meg videre. Jeg vil også utrette en stor takk til intervjuobjektene som stilte opp, og som ga utfyllende og gode besvarelser. Det har vært til stor hjelp underveis i oppgaven.

Jeg ønsker også å takke veileder Kirsti Berntsen for god oppfølging og gode, konstruktive tilbakemeldinger.

Trondheim 19.Mai

Emilie Forbord Dalen

Abstract

E-learning is a widespread tool in the workplace, and facilitates flexible competence building and training of both employees and managers. Through e-learning, learning can take place anywhere and anytime. Several businesses are currently developing e-learning packages for security training and awareness. Employee knowledge and awareness of cybersecurity is an important prerequisite for being able to safeguard information security. As information security not only requires increased awareness, but also a change in employee attitudes and behaviors, this study will investigate whether there are any aspects of digital learning that can affect employee attitudes, knowledge and behavior regarding information security.

This is investigated through the following question *"How can digital learning influence employees' knowledge, attitudes and behavior in relation to information security?".*

Sammendrag

E-læring er i dag et utbredt verktøy innen arbeidslivet, og tilrettelegger for fleksibel kompetansebygging og opplæring av både ansatte og ledere. E-læring bidrar til at læring kan foregå hvor som helst, når som helst. Flere eksterne aktører utvikler i dag e-læringspakker for sikkerhetsopplæring til de ansatte. Ansattes kunnskap og bevissthet om informasjonssikkerhet er en viktig forutsetning for å kunne ivareta informasjonssikkerhet. Ettersom informasjonssikkerhet ikke bare krever en økt bevissthet, men også en endring i de ansattes holdninger og atferd vil denne studien undersøke om det er noen aspekter ved digital læring som kan påvirke ansattes holdninger og atferd i forhold til sikkerhet.

Dette undersøkes gjennom problemstillingen *«Hvordan kan digital læring bidra til å påvirke de ansattes kunnskap,holdninger og atferd i forhold til informajonssikkerhet?».*

Innholdsfortegnelse

Innledning

Valg av tema

Informasjonssikkerhet har i takt med økende digitalisering av samfunn blitt mer aktuelt. Flere bedrifter velger å satse mer på IT, da dette kan bidra til økt effektivisering av flere forretningsprosesser. Samtidig øker det forventningene til digitalisering og det blir et krav fra flere kunder. Dette åpner derimot for nye trusler, som kan komprimere sensitiv informasjon som bedriften behandler, og som i flere tilfelle er vesentlig for å opprettholde den daglige driften. Nysgjerrigheten rundt dette tema kommer av at det til dags dato eksisterer et vidt tilbud av e-læringsprogram innen informasjonssikkerhet, som søker å øke de ansatte sin bevissthet om og kompetanse innen informasjonssikkerhet. Dette spiller en viktig rolle i å hindre virusangrep mot bedriften, da det er de ansatte selv som ofte utgjør den største trusselen. E-læring har i dag blitt et svært utbredt virkemiddel når det gjelder kompetansebygging i organisasjoner. Denne læringsmetoden gir fordeler i form av mer fleksibel læring, tilpasning til den enkelte og kan tilrettelegge for et godt læringsmiljø. Læring er en av de avgjørende faktorene når det kommer til endring av atferd. Kan e-læring derfor være bedre for ansattes atferd sammenlignet med tradisjonell læring/kursing? Basert på det vi finner av litteratur på temaet, kan det se ut til at e-læring er et underrepresentert området i forskning, da spesielt innenfor arbeidslivet.

Store aktører som NorSIS og Difi har b.la utviklet egne tilbud rundt kompetansebygging for både ledere og ansatte, som baserer seg på bruk av e-lærings moduler og andre digitale verktøy.

Slik kompetansebygging og bevisstgjøring har et overordnet mål om å sikre en god sikkerhetskultur. Jeg ønsker gjennom denne oppgaven å undersøke om e-læring kan ha noen virkning på hvordan de ansatte forholder seg til informasjonssikkerhet. Samtidig ønsker jeg gjennom egen empiriinnsamling å få en mer praktisk vinkling på hvordan sikkerhetsopplæring og e-læring håndteres i bedrifter.

Presentasjon av problemstilling

For å belyse dette temaet har jeg kommet frem til følgende problemstilling:

«Kan digital læring bidra til å påvirke ansattes kunnskap, holdninger og atferd i informasjonssikkerhet?»

Gjennom denne problemstillingen ønsker jeg å undersøke om det er aspekter ved e-læring som kan bidra til å påvirke kunnskap, holdninger og atferd i relasjon til sikkerhet.

Avgrensning og struktur av oppgaven

I den teoretiske delen vil det bli gjennomgått tidligere litteratur innenfor tema «læring» og «informasjonssikkerhet». Tema informasjonssikkerhet er avgrenset til området generell sikkerhetsopplæring, da det er denne aktiviteten hvor digital læring benyttes.

Case

For å kunne besvare problemstillingen er det tatt utgangspunkt i en virksomhet lokalisert her i Norge. Virksomheten refereres den til i denne oppgaven som «Bedrift A». Bedrift A er en stor organisasjon lokalisert i Norge, og består av 2000 ansatte. De har gjennomført oppdrag for flere internasjonale aktører, og er et av Europas største virksomheter innen sitt felt. Bedrift A har spisskompetanse innenfor flere områder, deriblant dem teknologi. Jeg hadde bekjentskap i Bedrift A fra før, og visste i denne sammenheng også at de hadde en sikkerhetskampanje, hvor e-læring ble brukt i sikkerhetsopplæringen.

Teoretisk grunnlag

Læring i organisasjoner

Læring i organisasjoner er ofte et komplekst område, da det ikke lenger er snakk om bare en person som skal lære, men en hel organisasjon bestående av flere individer. Det er derimot en nødvendig prosess for at organisasjonen skal kunne løpende tilpasse seg sine omgivelser. Spesielt er dette relevant innen informasjonssikkerhet, hvor både trusselbildet og virksomhetens omstendigheter er i stadig forandring. Dette vil kreve en bevisstgjøring som sørger for at de ansatte har den nødvendige kunnskapen til å kunne håndtere de truslene som møter dem i arbeidshverdagen, når de oppstår. Dette er også relevant med tanke på konkurransebildet, da ivaretagelse av informasjonens konfidensialitet, integritet og tilgjengelighet er viktig for å kunne opprettholde kundenes tillit.(Jacobsen & Thorsvik, 2016) Endring i omgivelsene tilsvarer på dette vis også en endring i organisasjonene, og Jacobsen & Thorsvik (2016) skiller, for denne form for endring, mellom planlagt og tilfeldig. Planlagt endring innebærer at organisasjonen evner å lære, slik at kontinuerlig evalueringer og vurderinger ivaretas ettersom det er en viktig forutsetning for læringsprosessen.
"Å studere læring i organisasjoner er å studere hvor fleksibel organisasjonen er."(Jacobsen & Thorsvik, 2016)
En del av utfordringene innen organisatorisk læring er at det kan være vanskelig å kartlegge *hvordan* læringsprosessen foregår hos det enkelte individ, da læring ofte kan skje ubevisst.(Jacobsen & Thorsvik, 2016)

Innen læringsteori skilles det mellom utvikling av kunnskap og ferdigheter. Da kunnskap er et abstrakt konsept, kan definisjonen av dette begrepet ofte være ganske diffust. Jacobsen & Thorsvik(2016) definerer kunnskap som *"innsikt i hvorfor noe fungerer eller skjer» og* ferdigheter som *«evnen til å bruke kunnskapen til å få noe til å fungere eller til å skje».* Læring er på samme måte som kunnskap også noe som er ulikt definert. I organisatorisk sammenheng har de ulike definisjonene en fellesnevner ved at de begge består av en handlings- og kunnskapsbasert faktor. Slik at læringsprosessen er noe som resulterer i en endring av atferd, og måten man praktiserer ting på.(Engvig, 2010, s.) For at læring skal finne sted på et organisatorisk nivå forutsetter det at det først skjer en læringsprosess på et individuelt nivå, og som individet mener er aktuelt for resten av organisasjonen. Deretter må denne kunnskapen spres til resten av de ansatte. Dette kan

foregå i form av aktiviteter som tilrettelegger for deling av erfaringer og kommunikasjon blant de ansatte. Intern kommunikasjon innad i organisasjonen er dermed en viktig faktor for kollektiv læring. Utfordringer, og det som ofte er en problemstilling i sikkerhetsopplæring, er at denne kollektive kunnskapen skal kunne resultere i en kollektiv endring av atferd.(Jacobsen & Thorsvik, 2016)

For å kunne nærmere undersøke hvordan læringsprosessen foregår, tar man ofte utgangspunkt i det som kalles taus og eksplisitt kunnskap. Taus kunnskap er den kunnskapen vi tar til oss ubevisst, og kan være vanskelig å sette ord på og formidle videre. Dette er kunnskap som har utviklet seg basert på erfaringer over lengre tid. På motsatt side finner man eksplisitt kunnskap som er anskaffet bevisst, og som kan beskrives med ord. I organisasjonssammenheng blir dette ofte dokumentert skriftlig og er med på å legge et grunnlag for rutiner og prosedyrer. Det er derimot den tause kunnskapen som skaper utfordringer i lærende organisasjoner, da mye av nøkkelen ligger i denne ubevisste kunnskapen hos de individuelle medlemmene.
Ved å analysere forholdet mellom eksplisitt og taus kunnskap har Jacobsen og Thorsvik(2016) identifisert fire former for læring som kan påvirke organisasjoner. Av disse formene nevnes det: sosialisering, eksternalisering, kombinering og internalisering. Sosialisering er en spredning av kunnskap mellom mennesker uten at dette gjøres bevisst. Det trenger heller ikke være noen form for kommunikasjon for at denne kunnskapen skal overføres. Sosialisering innebærer også at man kan lære ved å observere hverandre. Denne formen for læring har derimot sine ulemper da det forutsetter en fysisk tilstedeværelse. Samtidig er kunnskapen som anskaffes gjennom observasjon også taus, noe som gjør den vanskelig å ta tak i og behandle videre. For å gjøre om taus kunnskap til eksplisitt kunnskap, vil det være hensiktsmessig å se på eksternalisering. Ved hjelp av denne metoden kan taus kunnskap konkretiseres enten skriftlig eller muntlig, og kan deretter videreformidles til resten av organisasjonen. Kombinering retter seg mer mot å kombinere eksplisitt kunnskap for å kunne få et nytt perspektiv på situasjonen. På motsatt side av eksternalisering er det internalisering som handler om å gjøre eksplisitt kunnskap om til taus kunnskap.
Det er gjennom, aktiviteter som opplæring og bevisstgjøring at eksplisitt kunnskap formidles til medlemmer i organisasjonen.(Jacobsen & Thorsvik, 2016) Innenfor sikkerhet ønskes det at denne eksplisitte kunnskapen internaliseres, slik at de ansatte får en mer sikkerhetsorientert atferd.
Hvorvidt organisasjonen evner å tilegne seg ny kunnskap faller innenfor det Cohen og Levinthal(1990) betegner som absorpsjonskapasitet. I sammenheng med sikkerhet kan det tenkes at en lærende organisasjon kan ha en stor medvirkning i hvor effektivt sikkerhetsopplæringen er.

E-læring

Gjennom digital læring har nye metoder for læring blitt introdusert, og åpnet for en mer effektiv pedagogikk(Engvig, 2010, s.). E-Læring defineres som bruk av data- eller onlinebasert verktøy som skal tilrettelegge for læring. Målet ved denne form for læring er at man gjennom online-læring skaper et miljø hvor deltagere oppfordres til kunnskapsdeling og til engasjement i samarbeidende læringsaktiviteter.(Ghirardini, Food and Agriculture Organization of the United Nations, Germany, & Bundesministerium für Ernährung, 2011, s.)

Fordelene med e-læring er at det er lett tilgjengelig, og kan gjennomføres på brukernes vilkår. E-læring fjerner de geografiske begrensningene, ved at man kan lære hvor som helst, og når som helst. Kurs kan konstrueres på en måte som er mer engasjerende for brukere, ved å bruke multimedia presentasjoner eller interaktivt innhold. (Epignosis, 2014, s.) Brukeropplevelsen forbedres også ved at kurset kan gjennomføres i det tempo man selv ønsker. Sammenlignet med tradisjonell læring, kan e-læring være mer kostnadseffektivt da kostnader innenfor kursmaterialet, lokaler, instruktører bortfaller. (Engvig, 2010; Epignosis, 2014)Det er derimot ulik forskning på hvorvidt E—læring er mer effektivt sammenlignet med tradisjonell kursing.

Det er ulike metoder og materialer som kan benyttes når man legger opp et e-læringskurs. Innholdet i e-lærings kurs kan b.la bestå av: Enkle læringsressurser, interaktive e-leksjoner og elektroniske stimuleringer. Elektroniske simuleringer bygger på prinsippet om å lære ved å gjøre, da det er en stimulering av den virkelige verden og reelle situasjoner man kan komme ovenfor. Enkle læringsressurser kan omfatte presentasjon av tekst på nett, video, lydklipp, eller animasjoner. Dette krever lite aktivitet fra «elevens» side, da man kun behøver å lese, se og lytte. Denne form for e-læring har fordelen ved at det er enkelt og effektivt å utarbeide og legge ut. Opplæring kan derfor i denne formen raskt tilgjengeliggjøres for de ansatte, noe som kan være fordelaktig innenfor informasjonssikkerhet, hvor det stadig er endringer i trusselbildet (Ghirardini mfl., 2011)

E-læring kan også klassifiseres etter hvorvidt systemet er (lokal)datamaskin- eller internett-basert, også referert til som CBL (Computer Based Learning) eller IBL (Internet Based Learning) og WBL (Web-based learning). Datamaskinbasert læring omhandler hvordan bruk av installert programvare på datamaskinen kan benyttes til læring. IBL og WBL er derimot en videreutvikling av CBT (Arkorful & Abaidoo, 2014) WBL bruker derimot online kursinnhold, som kan tilrettelegge for asynkron og synkron kommunikasjon mellom brukere. Synkron kommunikasjon kan eksempelvis være gjennom chat, nettkonferanser og whiteboard. Asynkron kommunikasjon kan være innhold med link til epost, diskusjonsforum eller sosiale medier (Engvig, 2010)

E-læring i organisasjoner

E-læring blitt et utbredt verktøy for kompetansebygging i organisasjoner. Dette er typisk innenfor fagområder som IT, samt mellommenneskelige ferdigheter som teamarbeid, prosjektledelse og kommunikasjon. Det kan også brukes til opplæring av nyansatte. Mye av den opplæringen som tilbys hos bedrifter er tilrettelagt slik at de ansatte kan gjennomføre opplæringen på egenhånd. Dette vil si en selvstyring av når de ønsker å ta kurset, og når de ønsker å forlate det. Da det er fordelaktig for de ansatte å kunne regulere opplæringen selv, kan det derimot gi problemer i forhold til gjennomføring og deltagelse, da det tillater at man kan klikke seg kjapt gjennom, uten å ha ordentlig lest eller sett læringsinnholdet. (E. Derouin, Fritzsche, & Salas, 2005, s.)

Hvor effektiv e-læring er i organisatoriske sammenhenger er varierende. DeRouin et al (2005) benytter i sin studie 4 ulike metrikker for å måle effektiviteten av e-læring i organisasjoner: (1) Reaksjoner, (2) Læring, (3) Atferd og (4) Forretningsmessige resultat. I sin studie fant de ut at det var variert hvilken effekt e-læring hadde i forhold til

både reaksjon og læring. Ved å undersøke tidligere litteratur og forskning ble det derimot konkludert med at det var mulig for e-læring å påvirke atferd mer effektivt.

Det er derimot flere forutsetninger for å øke effektiviteten til e-læring. De nevner b.la at bruk av multimedia innhold i sammensetning med tekst var et viktig kriterium. Dette understøttes også av Engvig(2010) da hun i sin studie oppdaget en tydelig preferanse for videobasert innhold hos elever. Et annet viktig prinsipp DeRouin et.al (2010) påpekte var bruk av lyd der det passet seg. Grunnlaget bak dette prinsippet var at ansatte kunne bli for overveldet av visuell informasjon. Audio kunne bidra til en mer produktiv prosessering av informasjon, da lyd og visuell informasjon prosesseres i to forskjellige kanaler. Presentering av informasjon i ulike formater kan gi e-læring potensialet til å bli en effektiv opplæringsmetode. Det er derimot slik som de også påpeker at anvendelsen av e-læring i både organisasjoner og utdanning overgår den mengden forskning som er gjort på dette området. Slik at effektiviteten av e-læring er et område uten noe entydig og klart svar.(E. Derouin mfl., 2005)

Det er også en rekke barrierer som må tas i betraktning når e-læring skal implementeres i en organisasjon. For å forsikre seg om at disse barrierene kan overkommes, kan det være hensiktsmessig å måle hvor egnet en organisasjon er for at e-læring kan tas i bruk. Det bør b.la forsikres om at den teknologiske infrastrukturen er egnet til å distribuere læringsinnhold til alle ansatte. Hvor mye kapasitet som er nødvendig vil være avhengig av den enkelte organisasjonen og dens behov. Det bør også kartlegges om de ansatte har den nødvendige kunnskapen til å ta i bruk et nytt teknologisk verktøy. Det burde i denne sammenheng også forberedes for administrativ og teknisk støtte.(Schreurs, Ehler, & Moreau, 2008)

Flere organisasjoner tar også i bruk en læringsplattform, også kjent som LMS (Learning Management System), for å administrere e-læringskurs online. Dette gjør det b.la mulig å distribuere kurs gjennom internett eller intranettet til bedriften. Brukere får oversikt over tilgjengelige og fullførte kurs gjennom en kurskatalog. Et LMS gir også oversikt over påmelding og rapportering av hvilke kurs en bestemt brukergruppe har gjennomført.(Kvalnes, 2016)

NanoLæring

NanoLæring(bite-sized learning) er en metode innenfor e-læring som sørger for å formidle informasjon ved hjelp av korte 2-3 minutters leksjoner. Denne metoden ble utviklet som en respons på langvarige e-læringsleksjoner, som stilte krav til langvarig oppmerksomhet fra brukerne. Tradisjonelle e-læringskurs med varighet på mellom 30-60min ble gjennom tidligere forskning vist å være ineffektiv, da det førte til en overbelastning for hjernens evne til å fokusere og prosessering av informasjon, og som resulterte i at lærestoffet fort ble glemt. Hvor lenge vi evner å holde på informasjon er avhengig av kapasiteten til hukommelsen, og hvor lang tid som har passert etter man har fått ny informasjon.(Sian KOH, Gottipati, & Shankararaman, 2018)

Leksjoner med mye innhold, og som progresser i et raskt tempo skaper problemer for brukere, ved at de ikke får nok tid til å organisere egne tanker. Da digital læring tillater at læring følger et bruker-tilpasset tempo, vil en lang varighet fremdeles overskride arbeidsminne. I løpet av en læringsprosess er menneskets arbeidsminne begrenset, og at overskriding av denne kapasiteten kan skape hindringer for læring.(Sian KOH mfl., 2018)

E-læring bestående av langvarige leksjoner vil også skape hindringer i arbeidsdagen til de ansatte, ved at det kan være vanskelig å disponere tid til å gjennomføre leksjonene.

NanoLæring er en tilnærming som sørger for å optimalisere læringsprosessen, ved at den ikke bare er tilpasset den kognitive kapasiteten, men også de ansattes arbeidshverdag. Leksjonene kan gjennomføres når det passer den enkelte, og har en kort varighet. De ansatte behøver derfor disponere liten tid til læring, og kan fokusere på viktigere arbeidsoppgaver. Det har gjennom tidligere litteratur blitt gjennomført mer detaljerte undersøkelser på hvor effektiv denne metoden er. I en kvantitativ undersøkelse gjennomført av Sian et.al(2018) ble det identifisert et flertall fordeler ved NanoLæring sammenlignet med tradisjonell læring. Det ble også avdekket at NanoLæring var den foretrekkende læringsmetoden kontra den tradisjonelle. Det er derimot også ulemper ved denne metoden for læring. Noen tema krever derimot mer enn 2-3 minutter med innhold for at de skal kunne forstås. Informasjon som deles opp i små porsjoner kan være enkle å fordøye, men det kan være vanskeligere å identifisere sammenhengen mellom de ulike bitene av informasjon som presenteres. Det vektlegges derfor at utvikling av NanoLærings kurs bør sørge for at det er en tydelig sammenheng mellom de ulike modulene.(Trang, 2018)

Omer (2015) utpeker tre ulike faktorer bak utviklingen av NanoLæring. Den første omhandler et økende behov for mobil læring. Dette fordi det åpnet for en fleksibilitet, hvor de ansatte fikk mulighet til å gjennomføre læringskurs mens de reiste. Den andre faktoren var at læringsmetoden måtte bedre tilpasses menneskets evne til å fokusere. Den siste faktoren var et økende press på en raskere publisering og utvikling av e-læringskurs. For bedrifter er dette også et mer kostands-effektivt alternativ, da utviklingskostnader reduseres.(Omer Habeeb, 2015)
Det er flere materialer som brukes til å formidle innholdet i NanoLæring. Video har derimot hatt en økende utvikling innenfor NanoLæring, og har blitt et utbredt læringsmedium. Eades(2015) nevner flere årsaker til dette, hvor en av dem er at de fleste er visuelle lærere, noe som gjør video-basert læring til en populær metode.

Det er flere forretningsmessige fordeler ved å benytte seg av NanoLæring. En av dem inkluderer en økt effektivitet, da læring bruker en mindre tid av de ansattes arbeidshverdag, og etterlater mer tid til at man kan gjennomføre arbeidsoppgaver. Læringsinnholdet blir også delt inn i små porsjoner, som ikke etterlater mye plass til unødvendig og redundant informasjon. Læring blir også effektivt ved at man tar med den informasjonen som er mest relevant ovenfor det tema de ansatte skal lære, og man på denne måten "går rett på sak".(Sian KOH mfl., 2018)

Sikkerhetsopplæring og bevisstgjøring

I informasjonssikkerhet betegnes de ansatte ofte som den største trusselen.

«Informasjonssikkerhet er 20% teknologi og 80% holdninger»(Hjertø & Klefstad, 2018)

For å kunne etablere og opprettholde informasjonssikkerheten innad i en organisasjon er det vesentlig at de ansatte har den nødvendige kunnskapen og bevisstheten til å utføre

sine arbeidsoppgaver på en sikker måte. Opplæring og bevissthetstiltak bør sørge for en grunnleggende risikoforståelse hos de ansatte, samtidig som det bør kommuniseres hvorfor sikkerhet er viktig. Det bør også legges vekt på å motivere de ansatte til en mer sikkerhetsorientert tenking, i tillegg til at det foreligger en aksept og forståelse for de sikkerhetsmessige tiltak og regler som innføres. Et vellykket opplæringsprogram stiller også krav til at informasjonssikkerhet er godt forankret hos toppledelsen, og at programmet er forståelig for alle. Opplæringsprogrammet må også markedsføres på en måte som gjør den synlig for hele organisasjonen.(Daler, Gulbrandsen, Høie, & Sjølstad, 2010)Det understrekes også at det materiale som presenteres må være relevant for de ansatte., og at det benyttes flere kanaler for en effektiv formidling av informasjon. (PCI,2014) Slik at det ikke nødvendigvis er nok å *bare* benytte nettbaserte kurs, men at sikkerhet også kommuniseres ut til de ansatte gjennom e-post, intranett, plakater og postere.

Informasjonssikkerhet er et kontinuerlig og langsiktig arbeid. Det bør derfor foreligge en felles forståelse om at informasjonssikkerhet vil være et permanent fokus i bedriften. (Hjertø & Klefstad, 2018)Dersom sikkerhetskampanjen skal oppnå ønsket effekt, er det enkelte feller som burde unngås. En av disse er b.la knyttet til lite engasjerende og upassende læringsmaterialet. Opplæringsprogrammet burde heller ikke være sentrert rundt et enkelt område eller risiko, men vektlegge flere områder hvor det er behov for bevissthet og kompetanse. Eksempelvis burde ikke sikkerhetstrening og bevisstgjøring kun fokusere på e-post risiko, men også inkludere b.la trygg surfing på nett, ikke forlate PC'en ulåst osv.(Hjertø & Klefstad, 2018) Dette kan bidra til en felles forståelse om at sikkerhet er relevant på flere områder.

Motivasjon er et sentralt begrep når det kommer til læring. Forståelsen om hvorfor sikkerhet er nødvendig, og hvorfor man gjør det man gjør kan i seg selv være en motivasjonsfaktor.(Daler mfl., 2010) E-læring kan på dette området være et verktøy som kan bidra til økt personalisering og motivasjon, b.la gjennom bruk av gamification. Gamification handler om å benytte spillkonsept for å engasjere brukere i læring- og problemløsningsprosesser, og er en metode ofte benyttet for å øke motivasjon (Youssef, 2015) Tidligere forskning har derimot argumentert for at gamification ikke nødvendigvis fører til bedre tilegnelse av kunnskap, sammenlignet med mer tradisjonell læring. Allikevel ble kurset oppfattet som mer gøyalt og engasjerende (Youssef, 2015)Annen forskning har derimot funnet frem til at gamification kan ha en positiv effekt på læring, men at dette vil være avhengig av konteksten metoden benyttes, og hvilke brukere som gjennomfører kurset. (Garder B. Gjertsen, Gjære, Bartnes, & Rocha Flores, 2017)Det ble konkludert i samme rapport at flere brukere synes sikkerhetskurs var for langvarig, og at dette kunne ha negativ effekt på motivasjonen til å fullføre. Det ble også påpekt at selvbestemt læring resulterte i mer motivasjon. Da det er vanskelig å måle nøyaktig hvilken grad sikkerhetsopplæring påvirker atferd, konkluderte (Garder B. Gjertsen mfl., 2017) med at en jevnlig eksponering av opplæring og bevisstgjøring kan ha innvirkning på måten de ansatte tenker og kommuniserer rundt sikkerhet.

Sikkerhetsopplæring og atferd

Ved å se tilbake på tidligere litteratur, er det flere som stiller spørsmål til om sikkerhetsbevissthet og trening i det hele tatt har noen effekt på de ansattes atferd. Bada et. al (2014) konkluderer i sin studie med at opplæring og bevissthetstrening er

høyst nødvendig, men at det i seg selv ikke er nok til å endre atferd. Måling av sikkerhetsbevissthet, og hvordan opplæring og bevissthetsprogram påvirker atferd er derimot utfordrende å måle nøyaktig, da det er stor forskjell på hva man sier og hva man faktisk gjør.(Mathisen, 2004)

Haeussinger og Kranz (2013) definerer tre ulike perspektiver på sikkerhetsbevissthet: prosedyre, atferd og kognitiv. Det prosedyrebaserte perspektivet setter søkelys på utviklingen av opplæring og bevissthetstiltak, hvordan disse implementeres, og hvilken metode som benyttes. Fra det atferdsmessige perspektivet ser man nærmere på de faktorer som påvirker de ansattes intensjon til å samsvare med sikkerhetspolitikken. Det kognitive perspektivet går nærmere inne på tankesettingen til de ansatte rundt informasjonssikkerhet. Dette omhandler om hvorvidt de ansatte anerkjenner informasjonssikkerhet som et tema relevant for en selv og de rundt seg, og om det eksisterer en interesse om å lære mer slik at man kan utføre sine arbeidsoppgaver på en måte mer utrustet for angrep.

Ser man nærmere på organisasjonsteori kan også kultur i stor grad påvirke atferden til de ansatte.(Jacobsen & Thorsvik, 2016) Spørsmålet blir da om det må foreligge en god sikkerhetskultur for at sikkerhetsopplæring skal ha den ønskede effekten? Lafrance (2004) besvarer dette spørsmålet ved å definere sikkerhetskultur som et *«logisk resultat av et godt drevet sikkerhetsprogram»*. Alnatheers(2011) modell for evaluering av sikkerhetskultur understøtter også dette ved å utnevne sikkerhetsopplæring som en av de utgjørende faktorene for sikkerhetskultur.

Videre påpeker Gjertsen et.al (2017) at mer personalisert sikkerhetsopplæring og bevisstgjøring, i kombinasjon med praktiske øvelser, kan bidra til å øke sikkerhetsforståelsen og som resultat forbedre sikkerhetsatferden. Krebs (2014) argumenterer også for at digital læring kan endre atferd ved å skape minneverdige øyeblikk. Dette innebærer å benytte strategier og metoder som skaper følelser av lykke, selvtillit og felleskap. Basert på dette kan det tolkes som om sikkerhetsopplæring som vekker slike følelser, kan i større grad huskes av de ansatte.

KAB-modellen

Knowlede, attitude, behavior(KAB) er en metode som tar utgangspunkt i tre psykologiske faktorer for å evaluere effektiviteten av læring. Gjennom denne metoden ser man på hvordan kunnskap kan videre påvirke holdning og atferd. Anvendelse av denne metoden har derimot medbragt flere utfordringer i tidligere litteratur, da slike psykologiske faktorer kan være vanskelig å måle nøyaktig. Innenfor sikkerhetsopplæring er denne modellen ofte brukt som et utgangspunkt. (Khan, Alghathbar, Irfan Nabi, & Khan, 2011)

Kunnskap

Kunnskap kan defineres som *hva* man vet om noe, og det å vite *hvordan* man gjør noe. Et sentralt prinsipp i læring hos organisasjoner, er hvordan kunnskap kan tas tak i og videre behandles. Innen sikkerhetsopplæring settes det et læringsmål for det stoffet som skal gjennomgås. Hvordan en skal kunne evaluere om målet er nådd kan være en utfordring. Tidligere forskning har derimot rapportert at multiple-Choice, eller andre undersøkelser kan være effektive dersom de oppfyller visse betingelser. Disse

betingelsene innebærer at de spørsmålene som stilles er tydelige og lett forståelig. Slike prøver må også være konstruert på en måte som viser en tydelig sammenheng mellom lærestoffet som har blitt gjennomgått og spørsmålene som stilles i ettertid. De burde også være fri for elementer som kan distrahere brukeren.(Schrader & Lawless, 2004) Spørsmål stilt direkte etter stoffet er gjennomgått vil heller ikke nødvendigvis gi et korrekt bilde av hvor godt kunnskapen er innlemmet i et lengre tidsperspektiv. Slik at denne form for evaluering vil ikke si noe om hvor godt lærestoffet huskes.

Figur 1: KAB-modellen

Holdning

Informasjonssikkerhet omtales ofte som et holdningsskapende arbeid.(Hjertø & Klefstad, 2018) Holdninger kan i likhet med kunnskap ha flere definisjoner. I sin artikkel definerer Altmann(2008) holdning som et konsept bestående av kognitive, affektive og atferdsmessige komponenter, også kjent som ABC-modellen. Det kognitive leddet omfatter en tro eller ide mot et psykologisk objekt. Den affektive delen omfatter hvordan man evaluerer dette objektet, og hvilke følelser man har i tilknytning til det. Den atferdsmessige delen beskrives som den åpenbare handlingen rettet mot dette objektet. Hvilke av disse leddene som har størst rolle i utforming av holdning, kan være avhengig av en rekke faktorer. Petty et.al (1997) refererer til tidligere forskning, hvor det ble identifisert en sammenheng mellom autoritet og den kognitive og affektive delen av holdning. Det viste seg at de mer autoritære hadde en holdning drevet av symbolske trosretninger og tidligere erfaringer. På motsatt side, var de mindre autoritære mer drevet av affekt og stereotypisk tro. Det kan ut ifra dette eksempelet virke som det er individuelt hvilke av de tre leddene som bestemmer holdning.

Hvor *sterk* en holdning er involverer flere faktorer. Dersom en holdning har høy betydning for egeninteresse, sosial identitet og verdi vil dette være veldig viktig for en selv. I forhold til KAB-modellen, kan kunnskap og forståelse også definere hvor sterk en holdning er. Hvor mye kunnskap man har om et objekt kan fortelle noe om holdningen til det aktuelle objektet.
"*People are generally more knowledgeable about topics that interest them and are likely to hold strong attitudes (positive or negative) as a consequence"* (McLeod, 2018)
I samme artikkel nevnes det også at holdninger som utformes av egne erfaringer ofte har høyere betydning for et individ, sammenlignet med de holdninger som utformes indirekte, det vil si gjennom det vi leser, hører eller ser på tv.(McLeod, 2018) Ser man dette i sammenheng med informasjonssikkerhet kan det derimot tenkes at de som har opplevd eller erfart situasjoner hvor IT-sikkerheten har blitt kompromittert, vil utforme en sterkere holdning sammenlignet med de som bare leser og blir fortalt at informasjonssikkerhet er viktig.

Måling av holdninger innad i en organisasjon er derimot komplekst, da det er flere aspekter som må tas i betraktning. Det er i denne sammenheng også vanskelig å avgjøre hvordan holdning kan bidra til å forutsi atferd, da holdning er en funksjon av den situasjonen den forekommer i. (Schrader & Lawless, 2004)

Atferd
Atferd defineres av Malt (2019) som *"den totale personlige eller gruppemessige menneskelige oppførsel og uttrykksform som preges av det herskende kulturmønster på en bestemt tid og et bestemt sted".* McLeod (2018) påpeker at holdninger kan bidra til å forutsi atferd. Allikevel er ikke menneskets atferd alltid konsistent med egne holdninger. Det er de holdningene som er av høy betydning for oss som har best sannsynlighet for å forutsi atferd.(McLeod, 2018)

For å få et bilde av noen eller en gruppe mennesker sin atferd, krever dette som oftest observasjoner over lengre tid. Tidligere forskning har benyttet flere metoder for å vurdere atferd. Det har blitt forsøkt å bruke mer direkte metoder, ved å analysere forekomsten av en bestemt atferd eller handling innad en viss tidsperiode. Intervju er b.la også en metode brukt for å vurdere atferd. (Schrader & Lawless, 2004)

Modellen kan derimot vise seg å være mer dynamisk enn antatt, da de ulike komponentene kan ha en gjensidig påvirkning på hverandre. Det kan for eksempel være et forhold mellom atferd og holdning, i den forstand at en bestemt atferd kan påvirke følelser man får tilknyttet et psykologisk objekt. Kunnskap utgjør heller ikke den eneste faktoren i endring av atferd. (Schrader & Lawless, 2004) Khan et.al (2011) velger å utvide modellen ved å benytte andre faktorer som subjektive normer og intensjoner for å evaluere effektiviteten til ulike opplæringsmetoder. Disse faktorene innlemmes på grunnlag av en teori referert til som TPB (Theory of Planned Behavior), som beskriver intensjon som en av de utgjørende faktorene for endring i atferd. Intensjon var videre påvirket av faktorer som holdning og subjektive normer. Subjektive normer vil tilsvare hvordan en person tror andres tanker om en vil påvirkes dersom en bestemt atferd utføres. Khan konkluderte med at CBT (computer based training) hadde lav effekt, da det sosiale og det intensjonelle leddet var fraværende, og at det på denne måten mislykket i å påvirke atferd. Komponentet til å endre holdning og til å påvirke kunnskap var derimot tilstede.

Metode

For å kunne svare på problemstillingen er det hensiktsmessig å samle inn egen empiri, som kan bidra til å belyse tema fra et brukerorientert og et utviklings/ledelsesorientert perspektiv. Valg av forskningsdesign, metode og datainnsamling er beskrevet i dette kapittelet. Kvalitetssikring av innsamlede data vil beskrives i form av pålitelighet, gyldighet og overførbarhet.

Forskningsdesign

Av forskningsdesign skilles det mellom intensivt og ekstensivt design. Et ekstensivt design baserer seg på datainnsamling fra mange kilder, men består som regel av få variabler. Dette er ofte et design hvor det benyttes kvantitativ metode for datainnsamling. I et intensivt design fokuseres det på flere variabler, men da ofte få kilder.(Busch, 2013) Denne oppgaven vil først og fremst følge et intensivt design, da det

samles informasjon fra et fåtall kilder i form av et dybdeintervju, etterfulgt av såkalte speed-intervju av en gruppe ansatte .

Problemstillingen var i utgangspunktet sentrert rundt sammenhengen mellom digital læring og sikkerhetskultur. Etter gjennomføring av intervju var det derimot behov for å rekonstruere problemstillingen, da intervju ikke er den best mulige metoden for å kartlegge sikkerhetskultur. For å kartlegge sikkerhetskultur har det vært hensiktsmessig med observasjoner over en lengre tidsperiode.

Til denne oppgaven har jeg valgt et intensivt design, med en kvalitativ metode for datainnsamling. Dette designet er valgt med tanke på at problemsstillingen kan besvares best ved å samle inn informasjon som går mer i dybden på temaet. Samspillet mellom mennesket, teknologi og organisasjon er et komplekst område, hvor det er behov for å analysere flere variabler for å best mulig kunne belyse temaet, og identifisere sammenhenger. Det vil allikevel ikke kunne defineres noen universell regel som vil være gjeldende for andre individer og organisasjoner, dette p.g.a at menneskets atferd er såpass komplekst, og det som er gjeldende for noen behøver ikke være gjeldende for andre (Jacobsen & Thorsvik, 2016) På dette området har ekstensive og kvantitative forskningsdesign vært fordelaktig å supplere med, da det kan bidra til å identifisere om det er noen reaksjoner/tankeganger som forekommer oftere, som deretter kan identifisere et kollektivt mønster.

Valg av forskningsmetode

For å få kunne belyse problemstillingen best mulig, var det hensiktsmessig å samle inn egen empiri som kan supplere til allerede eksisterende teori. Jeg har derfor valgt å benytte meg av en kvalitativ forskningsmetode i form av intervju.

Intervju er en kvalitativ metode som anvendes med hensikt om å samle dypere begrunnelser av informantene. Det vil i denne oppgaven gjennomføres 5 en-til-en intervju. Det er ulike måter intervjuet kan utføres. Mannion (2007) kategoriserer mellom tre ulike metoder: standardisert, semi-standardisert og ustandardisert. Et standardisert intervju inneholder spørsmål strukturert i en rekkefølge som følges i løpet av intervjuet. Dette ansees som en mer formell intervjumetode, og etterlater ikke plass til at det snakkes om emner utenom det som inngår i intervjuet. Ved å benytte en semi-standardisert metode benyttes det en fastsatt struktur over tema som skal besvares, men tillater at informanten kan komme med uforutsette innspill og besvarelser. Ustandardisert metode er en uformell metode, hvor det brukes en guide med mer åpne spørsmål eller tema som kan bidra til å skape en samtale. Gjennom denne metoden blir det lagt opp til at den som utfører intervju følger informantens retning.

En-til-en intervju kan gjennomføres ansikt-til-ansikt eller gjennom telefon eller eksempelvis Skype. Intervju som gjennomføres ansikt-til-ansikt åpner for at ikke-verbal kommunikasjon kan plukkes opp, og gi en dypere forståelse av det som blir sagt.(Mannion, 2007) Til denne oppgaven er det benyttet en semi-standardisert metode, som gjennomføres ansikt til ansikt. Dybdeintervjuet var planlagt å gjennomføres først, da besvarelser og innspill i forhold til leksjonene og sikkerhetskulturen kunne gi videre grunnlag til spørsmål hos de ansatte.

Intervjuguide

Intervjuguiden ble utarbeidet med hensyn til problemstillingen og tema i oppgaven. Det ble tatt utgangspunkt i en mal gjort tilgjengelig gjennom emnegruppen på skolens læringsportal. Denne malen ble videre tilpasset de tema som skulle undersøkes i oppgaven, og ble delt inn i en tematisk struktur. Intervjuguiden ble deretter inndelt i tema «e-læring» og «informasjonssikkerhet». Etter datainnsamlingen var gjennomført, i tillegg til en videre litteratursøking, ble det nødvendig å innsnevre problemstillingen, ved å fokusere mer spesifikt på digital læring innen sikkerhetsopplæring, da sikkerhetskultur ble på et for overordnet nivå. Det ble derfor lagt hovedfokus på om digital sikkerhetsopplæring kan bidra til å endre ansattes kunnskap, holdninger og atferd i forhold til informasjonssikkerhet.

Utvalg av informanter og gjennomføring av intervju

Til dybdeintervjuet ønsket jeg å intervjue noen med kompetanse innenfor informasjonssikkerhet, slik at det var mulig å høre informantens tanker rundt tema og problemstillingen. Jeg ønsket i denne sammenheng også et mer praktisk innblikk i hvordan informasjonssikkerhet, da spesielt sikkerhetsopplæring, håndteres i bedrifter. På bedriftens hjemmeside var det oversikt over ansatte innenfor det aktuelle fagområdet med kontaktinformasjon. Forespørsel om vedkommende kunne delta i intervju ble sendt via epost. Vedkommende hadde mulighet, og tid og sted for gjennomføring av intervjuet ble avtalt.

For de ansatte var det ingen utvalgskriterier annet enn et ønske om å delta i intervjuet. Jeg hadde bekjente i den utvalgte bedriften som spurte kollegaer på sin avdeling om noen var interessert i å delta på intervju. De som hadde mulighet til å delta ble kontaktet via epost, slik at dato og tidspunkt for gjennomføring av intervjuet kunne avtales. Alle de ansatte i intervjuet hadde en relativt lik teknisk kompetanse og bakgrunn. Det ble i utgangspunktet utvalgt 4 ansatte som skulle besvare de samme spørsmålene, dette for å få ulike synspunkt og meninger fra brukernes perspektiv. En av de ansatte hadde derimot deltatt i utvikling av leksjonene, slik at det på denne måten ble vanskelig å få et brukerorientertperspektiv. Informanten hadde en faglig bakgrunn innen pedagogikk, og mye nyttig informasjon i forhold til e-læringsleksjonene, i tillegg slik at dette ble omgjort til et supplerende dybdeintervju. Videre i oppgaven vil «informant» være betegnelse på de som deltok i dybdeintervjuet, og «ansatte» er betegnelsen på de som stilte opp til speed-intervjuene

Intervju	**Antall informanter**	**Varighet**
Dybdeintervju	2	20-30 min
Speed-intervju	3	5-10 min

Alle intervjuene ble gjennomført på et tilgjengelig møterom hos Bedrift A. For det første dybdeintervjuet ble det satt av en time. Intervjuguiden var et nyttig hjelpemiddel, men ble ikke fulgt slavisk. På den måten kunne jeg stille oppfølgingsspørsmål til de innspill og beskrivelser som informanten kom med. Det ble først tatt utgangspunkt i «e-lærings» temaet. Innenfor dette tema ble det stilt spørsmål i forhold til oppbygning av e-læringskursene, om de var obligatoriske, om effekten av de evalueres og om det ble

tilbudt annen opplæring til ansatte mer involvert i bruk av IT-systemer. Det ble også gjennom disse spørsmålene gitt beskrivelser av den overordnede sikkerhetskampanjen. Under tema rettet mer mot informasjonssikkerhet ble det stilt spørsmål mer relatert til bakgrunnen for sikkerhetskampanjen og om intervjuobjektet hadde noen tanker rundt problemstillingen.

For gruppen med de ansatte ble det i utgangspunktet planlagt å intervjue 4 stk. Intervjuene ble gjennomført hver for seg og det ble satt av 10-20 min for hvert intervju. Alle ansatte hadde mulighet til å stille opp på samme dag. Det ble benyttet samme tematisk struktur som i dybdeintervjuet. E-læringstemaet inneholdt spørsmål tilknyttet de ansattes opplevelse og oppfatning av leksjonene. Neste tema inneholdt spørsmål nærmere tilknyttet hvilket forhold de hadde til informasjonssikkerhet før leksjonene ble gjennomført, dette for å kartlegge om leksjonene eventuelt hadde ført til en økning i bevissthet og kunnskapsnivået.

Dataanalyse

Når det kommer til dataanalyse er det flere metoder som kan anvendes. Innenfor kvalitative forskningsmetoder kan det benyttes en form for systematisk meningskategorisering, mens andre metoder setter søkelys på å hente ut gode beskrivelser og fortellinger (Busch, 2013)Hvilken metode som benyttes kommer an på de data man har samlet inn gjennom forskningsmetoden. I denne oppgaven har det blitt benyttet en blanding av begge metodene. Under analyse av dybdeintervjuene ble det brukt fargekoding til å kategorisere de ulike sitatene etter tema informasjonssikkerhet eller e-læring. Denne metoden gjorde det også mulig å utheve de sitatene som var mest relevant for videre drøfting og besvarelse. Analyse av datainnsamlingen fra de ansatte ble ikke inndelt i tema, men sørget mer for å utheve de mest relevante sitatene og besvarelsene i forhold til de spørsmålene som ble stilt.

Metodekvalitet

Metodekvalitet forteller noe om undersøkelsens kvalitet, og om de resultatene som fremkommer kan stoles på. Kvaliteten måles i tre ulike dimensjoner: (1) Pålitelighet, (2) Gyldighet og (3) Overførbarhet. Pålitelighet omhandler i hvilken grad man kan stole på de dataene som er kartlagt. I kvalitative metode vil den som utfører forskningen alltid ha en innvirkning på det datamaterialet som samles. Det blir gjennom kvalitativ metode derfor vanskelig å gjennomføre samme forskning med et identisk resultat. (Leseth & Tellmann, 2018) Det var derimot i denne oppgaven ingen relasjon mellom forsker og intervjuobjektene som kunne påvirket resultatene.

Gyldighet handler om i hvilken grad man undersøker det man skal undersøke. (Busch, 2013)Det skilles mellom begrepsvaliditet og intern validitet når det diskuteres hvor gyldig forskningen er. Begrepskvalitet forteller noe om teorien man bruker og det man måler samsvarer. Intern validitet forteller derimot noe om det produserte datamaterialet faktisk forteller noe om det fenomenet som skal måles.(Leseth & Tellmann, 2018) På grunn av endringer og omformulering av problemstilling etter gjennomført empiri, har dette påvirket både begrepsmessige og interne validiteten. Teorigrunnlaget gikk fra å handle om sikkerhetskultur til å gå mer spesifikt inne på sikkerhetsopplæring. Dette ble videre utviklet til å ta utgangspunkt i KAB-modellen, som i tidligere forskning er et grunnlag for evaluering av sikkerhetsopplæring sin effekt på atferd. Etter å ha fått mer kjennskap til modellen, var også noen av spørsmålene stilt under intervjuet mindre relevante.

Informantene ga derimot gode og utfyllende svar, som fortsatt kunne tas tak i til å besvare den omformulerte problemstillingen. Dersom intervjuet skulle blitt gjennomført på nytt hadde jeg derimot stilt noen andre spørsmål, som bedre kunne si noe om holdning, atferd og kunnskap i relasjon til digital læring.

Overførbarhet sier noe om i hvilken grad forskningen kan overføres til andre situasjoner. (Busch, 2013)Det ble i denne undersøkelsen kun tatt utgangspunkt i noen få ansatte. Overførbarheten blir i denne sammenheng også preget av at de ansattes følelser i relasjon til opplæringen ikke er felles for hele organisasjonen. Noe av de dataene som fremkommer belyser derimot flere fordeler ved e-læring innenfor sikkerhetsarbeid som kan være relevante.

Resultater

Presentasjon av e-læringsleksjonene

E-læringsleksjonene innenfor sikkerhetskampanjen består av en sammensetning av videosnutter og tekstlige beskrivelser. Videosnuttene har en varighet på 1 minutt. Hver modul tar for seg et enkelt tema f.eks deling av dokumenter, spam epost, låsing av pc osv. Videosnuttene bruker egne ansatte som skuespillere hvor de illustrere et scenario eller en uheldig situasjon som de ansatte kan møte på i sin arbeidshverdag. Videoen blir etterfulgt av 5-10 slides med en tekstlig forklaring. Bedrift A kjører 2 måned i året hvor det legges ekstra vekt på IT-sikkerhet. I løpet av denne måneden publiseres det 4-5 videoleksjoner, som legges ut tilgjengelig for de ansatte. Leksjonene er tilgjengelige hele tiden, men er ikke obligatoriske å gjennomføre. Leksjonene følger metoden nanolæring hvor leksjonene er korte, og kan lett gjennomføres i løpet av en arbeidsdag.

Leksjonene er også konstruert slik at de viktigste læringsmålene kommer frem i løpet av de korte leksjonene. Videre er det lagt vekt på at videosnuttene har en humoristisk sans.

> *«Som skal på en måte skape spenning og humor i det hele, få til en snakkis rundt det, av og med Bedrift A-folk. Så det har vært en del av gangen i det tenker jeg, og det at de tingene vi tar opp det er noe hver og en kan relatere seg til.»*- Informant 2

Utgangspunktet for leksjonene var basert på et sett med generelle leksjoner fra en ekstern leverandør. Innholdet i disse leksjonene var på et generelt nivå, men var ikke tilpasset den enkelte bedriften.

> *«Og det var typisk bare sånne slides og litt tekst du kunne klikke deg gjennom. Ikke noe galt i det, men veldig generelle tekster. Så det vi endte opp med å gjøre var å skrive om, endret nesten alt, for å få det til å passe til Bedrift A regler og Bedrift A sin hverdag. De var et godt utgangspunkt, det var ikke noe feil i dem. Men vi måtte tune litt for å gjøre det relevant.»* - Informant 1

Sikkerhetskampanjen var basert på et behov om mer generell sikkerhetsopplæring, da det i en periode var et tema som ikke ble snakket så mye om.

> *«Vi trengte å gjøre et eller annet for å kommunisere til folk hva truslene er, hva er deres ansvar og hvilke situasjoner kan de komme opp i, og hva gjør du med dem.»* - Informant 1

Det er også viktig å påpeke at e-læringsleksjonene kun utgjør en del av sikkerhetskampanjen, og at det er flere faktorer og tiltak som eksisterer parallelt og som kan bidra til å påvirke de ansattes forhold til sikkerhet. Det ble b.la brukt iverksatt diverse motivasjonstiltak som kakekonkurranser og utdeling av diplom for fullførte leksjoner.

> *«Den hang folk opp på kontordøren sin, og så var det en kakekonkurranse i bakant og litt andre ting som kaffekopper, buttons, musematte eller hva det ikke var. Så da er det klart at du brander det på en annen måte som skaper bevissthet hos folk.»*-Informant 2

I etterkant av sikkerhetsmåneden har det blitt gjennomført frivillige spørreundersøkelser som de ansatte har hatt mulighet til å svare på. Dette har derimot siktet på å evaluere sikkerhetskampanjen som en helhet ved å gjennomføre kunnskapstester i tillegg til andre observasjoner, men ikke noe som forteller om effekten av e-læring spesifikt. Ved hjelp av intervju med noen få ansatte, er det mulig å få en dypere begrunnelse på selve brukeropplevelsen av leksjonene og om de har noen påvirkning på kunnskap, holdning og atferd i informasjonssikkerhet.

> *«Vi har sett en tydelig utvikling fra år til år. Folk har lært litt mer og skjønt litt mer hvorfor dette er viktig»* -Informant1

Det har ikke blitt brukt noen form for tradisjonell klasseroms kursing i dette tema tidligere. Men det nevnes derimot at det arrangeres avdelingsmøter hvor tema IT-sikkerhet står på agendaen.

> *«For noen så er det veldig mye bedre. For det gir rom for å stille spørsmål og så gir det rom for å få ut litt frustrasjon, fordi noen er irritert og synes at «uff, hvorfor skal vi bruke denne løsningen den er så dårlig.»*

Selv om e-læring er i rask utvikling og er i dag et vanlig verktøy for kompetansebygging, gir utdraget ovenfor et eksempel på en av fordelene ved tradisjonell kursing som kan være vanskelig å få gjennom e-læring.

Intervju av de ansatte

E-læringsleksjonene

Av de ansatte er det blitt stilt spørsmål sentrert rundt deres oppfatning og tanker om e-læringsleksjonene, og eventuelle tanker om noe de skulle ønske var annerledes. Følgende sitater er samlet etter spørsmål om hva de synes om e-læringsleksjonene.

Ansatt 1	**Ansatt 2**	**Ansatt 3**
«Jeg synes de er veldig bra mye fordi at de er så korte. At da er det så enkelt å ta dem. Og så er det veldig greit å ta de sånn innimellom. veldig sånn to the point, og veldig enkel og forklarende for meg. Jeg er ikke så god på IT, sånn teknisk og jeg spør om hjelp. Men jeg synes de leksjonene var enkel nok til at vi som ikke har så mye teknisk begrep at vi også forsto det. Det at de brukte ansatte i videoer og sånt gjorde at det ble veldig gøy. Den gjenkjennelsen i tillegg, til at du skjønte hva det var snakk om. De klarte å få oppmerksomheten da.»	*«Det som jeg kanskje synes er finest med de e-læringene er at det er video der. At det ikke bare er en eller annen tekst som skal leses, så skal du huske hva det var, så kommer det spørsmål etterpå. Så akkurat den biten med video gjør det mer interessant. Og litt lettere å kanskje huske og relatere seg til når de har hentet ut konkrete eksempler fra hverdagen i Bedrift A da.»*	*«Jeg har jo sett flere omganger, men kan jo innrømme at jeg tror ikke jeg har fullført den siste som ligger der. Jeg synes det er veldig artig at de bruker humor, veldig bra pedagogikk. Så jeg husker ting etterpå. Det blir fort kjedelig med pekefinger. Jeg er sikker på at man husker det bedre når det er underholdende. Så jeg liker veldig godt den formen. At de får formidlet det effektivt, det synes jeg.»*

Ansatt1 utpeker varigheten, formidlingen, og videoen som viktige elementer til at leksjonene oppfattes positiv. Det at det brukes video utpekes også av Ansatt 2 som en viktig del av leksjonene, og som bidrar til å skape interesse og holde på oppmerksomheten. Ansatt 3 påpeker at det er humoren i videoene som er det viktigste faktoren til at leksjonene fanger oppmerksomheten og at man husker læringsstoffet. Ansatt 2 sikter også til det faktum at det er relaterbart som en viktig del av den totale effekten til leksjonen. Da tilgjengelighet ofte utpekes som en av de mest positive sidene ved digital læring, var neste spørsmål relatert til hvorvidt de ansatte går tilbake til leksjonene dersom det skulle oppstå usikkerhet rundt noen av temaene.

Ansatt 1	Ansatt 2	Ansatt 3
«Ja, jeg tror ikke jeg har gått tilbake på noe. Burde vært repetert annethvert år. Særlig hvis man ikke er borti noen av tilfellene, hvis man ikke har så mye med sånt å gjøre, så er det fort gjort å glemme det. Så jeg tror kanskje at jeg ville repetert kampanjen om et år eller to.»	*«Ja, nei egentlig ikke. Men det har jo absolutt hjulpet på å få en økt bevissthet og kunnskap om det. Det som jeg kanskje husker mest er å lukke pc'en og sånn, ikke bare la den stå åpen. For det har jeg aldri tenkt på egentlig, før jeg kom hit at det kan være et problem. Men jeg synes i alle fall det har vært bra på å øke bevisstheten rundt det.»*	*«Går tilbake- nei det har jeg aldri gjort. Jeg vet ikke om det kommer noen spørsmål til min holdning mot sånne regler, men jeg er livredd for å gjør noe galt.»*

Dette så derimot ikke ut til å være nødvendig, da igjen av informantene har hatt noe behov for å gå tilbake. Ansatt 2 påpeker at leksjonene har bidratt til å skape en økt bevissthet og kunnskap rundt emne sikkerhet.

Forhold til informasjonssikkerhet

Neste spørsmål ble stilt i forbindelse med den opprinnelige problemstillingen, men besvarelsene hadde mye relevant informasjon i forhold til hvordan de kommuniserte om informasjonssikkerhet.

Ansatt 1	Ansatt 2	Ansatt 3
«Ja, for vi snakker jo om slike ting til lunsj og på møter og allmøter så har vi også snakket om slikt innimellom. Når det er noe som er aktuelt da, så hender det vi snakker om det, og da begynner vi å spørre om det i Bedrift A sammenheng. «Nå ser jeg at det er en bedrift med sånn og sånn, hvordan er det hos oss?»	*«Jeg tror det ble en snakkis rundt «har du sett den siste leksjonen, med det og det temaet, der den og den ble lurt?» Bedrift A består jo av 2000 stykker, så det er klart at alle kjenner ikke alle, men mange kjenner mange. Og hvis man da vet av noen som har vært med på en innspilling, så liksom blir jo det ekstra gøy. I tillegg til den kakekonkurransen gjør jo at folk snakker om det «kom igjen ta den leksjonen, har du ikke tatt den enda? Vi vil jo vinne, hallo vi skal jo bli best» så det konkurranseelementet*	*«Ja, når de kommer så blir det det. Fordi de er morsomme.»*

	tror jeg også fungerer veldig bra, som bidrar til at det blir en snakkis i avdelingene og i faglaget.»	

Første informant nevner ikke noe om videoleksjonene spesifikt, men at informasjonssikkerhet er et samtaleemne i lunsj og møtesammenhenger. Samtaler rundt informasjonssikkerhet i nyhetsbildet og hvordan dette relateres til informasjonssikkerhet i egen bedrift tyder på at det eksisterer en interesse for emnet og hvordan egne/andres ansvarsroller relateres til uheldige situasjoner som kan oppstå dersom det skulle hende noe i egen bedrift. Ansatt 2 og 3 refererer derimot nærmere til videoleksjonene, og at inkluderingen av ansatte ofte fører til at det blir et samtaleemne, og at det også på denne måten kan oppfordres til at andre ansatte tar leksjonen. Konkurranseelementet er også her en annen faktor som er med på å gi leksjonene oppmerksomhet, og en mulig motivasjonsfaktor til å gjennomføre leksjonene. Det blir derfor i denne sammenheng vanskelig å si hvilket element som har størst effekt, men Ansatt 3 understøtter at humoren er en viktig faktor i å skape samtaler rundt leksjonene og informasjonssikkerhet.

At formidlingen er gjort såpass forståelig for de som ikke har et stort teknisk begrep sikter mer til et godt pedagogisk valg, heller enn at det er digitalt. Det er derimot varigheten på kursene, at de er korte og kan gjennomføres innimellom som viser et noe unikt ved digital læring, da også innenfor den formen som kalles nanolæring.

For å kartlegge om leksjonene har nådd sitt mål i å øke bevisstheten, var det også hensiktsmessig å forhøre litt mer om kunnskapsgrunnlaget til informantene når det gjelder informasjonssikkerhet, og derfor også litt om atferd under gjennomføringen av leksjonene. Dersom mye av kunnskapen og bevisstheten er tilstede fra før gir digital læring fordelen ved at man kan gjennomføre det i eget tempo.

Ansatt 1	**Ansatt 2**	**Ansatt 3**
«Ja, noe av det visste jeg. Men jeg synes det var veldig greit å få det i de korte leksjonene. Men noe av det visste jeg fra før, men noe var nytt for meg.»	*«Nei, mye av det er jo ting man vet fra før av. Men som man ikke har et like bevist forhold til før man tar de kursene om hvorfor det er viktig. Det er kanskje det som er mest nyttig, å få det forklart hva som kan skje hvis du ikke passer på det og det, bli obs på ting som kan skje, eller måter folk kan lure deg på.»*	*«Ja, særlig det med å åpne vedlegg. Det er noe jeg har blitt fortalt fra dag 1.. Det visste jeg fra før. Det var det jeg skjønte var noe av det viktigste, og ikke åpne vedlegg. Jeg er med å skrive populærvitenskapelige artikler om datasikkerhet og hva som er de vanligste fellene osv. Så derfor vet jeg litt om det den veien også. og så har jeg lært litt nye ting. Så alt var ikke helt nytt.»*

Alle informantene hadde en grei bevissthet i forhold til standard sikkerhetsregler som det å ikke åpne vedlegg, samt eposter osv. Mye av denne forkunnskapen var et resultat av en involvering i arbeid med sikkerhet. Informant 1 og 2 presiserte at til tross for den grunnleggende bevisstheten, var leksjonene også med på å skape økt bevissthet rundt ny type informasjon. Det påpektes også at denne bevisstgjøringen gjør at man er oppdatert på de nye metodene kriminelle tar til for å lure ansatte. Ansatt 2 nevner også at det ligger mye verdi i forklaringen på «hvorfor» man må følge retningslinjer og rutiner i forhold til eks e-post, dokumentdeling osv. Samme informant nevner også at graden av bevissthet øker ved at slike leksjoner gjennomføres. De ansatte oppfattet eget bevissthetsnivå som tilfredsstillende, men at mye av dette også var forårsaket av involvering i sikkerhetsarbeid og ikke nødvendigvis e-læringsleksjonene.

Dybdeintervju

Gjennom dybdeintervjuene har det blitt lagt fokus på å få mer innsikt inn i sikkerhetsopplæringen og kulturen fra ledelsen og utviklernes side. Det ble i intervjuguiden delt mellom to tema: e-læring og sikkerhetskultur. Informant 1 tilsvarer den sikkerhetsansvarlige, og Informant 2 tilsvarer den med bakgrunn i utvikling av e-læringsleksjonene.

E-læring

Spørsmålene rundt e-læring sentrerer seg rundt hvordan de er lagt opp, og litt om begrunnelsene til de valgene som er tatt. Leksjonene er utarbeidet av Bedrift A sin egen avdeling for kompetansebygging. Dette er gjort etter forespørsel fra IT-ledelsen som har da identifisert et behov for å øke bevisstheten rundt sikkerhet.

Leksjonene inneholder interaktivitet i den form at man kan klikke seg videre gjennom den tekstlige forklaringen. Dette gjør at læringen kan tilpasses de ansatte ut ifra deres grunnleggende bevissthets- og kunnskapsnivå, slik at leksjonene kan gjennomføres i eget tempo. En ulempe ved dette som også introduseres gjennom dybdeintervjuet er b.la at de med lite bevissthetsgrunnlag også kan klikke seg kjapt gjennom leksjonene, og dermed forårsake at det ikke har noen effekt. Bedrift A hadde ikke benyttet seg av noen tradisjonell form for kursing innen informasjonssikkerhet tidligere. Det ble derimot arrangert avdelingsmøter som ga noe av de samme fordelene som tradisjonell kursing.

> *«For noen så er det veldig mye bedre. For det gir rom for å stille spørsmål og så gir det rom for å få ut litt frustrasjon, fordi noen er irritert og synes at «uff, hvorfor skal vi bruke denne løsningen den er så dårlig». Så kan du stå der og svare ut og forklare, og så kan det gjøre at de blir litt mindre frustrert. Og så hører alle det, så det er med på å dempe den generelle frustrasjonen i gruppa for eksempel. Så det kan ha en positiv effekt. Så er det andre som føler at «jeg kaster bort tiden for jeg vet det fra før» men de må sitte der fordi de er pålagt til å sitte der.»* Informant1

«Relevans» og «humor» er to nøkkelord som ser ut til å være viktig fra både de ansatte og utviklingens perspektiv. Det finnes i dag flere e-læringspakker på nettet fra eksterne aktører, som da ofte spesialiserer seg innenfor utforming av e-læringskurs. En ulempe ved dette er at det kan ofte bli for generelt, og ikke tilpasset bedriften. En konsekvens av dette kan være at det skaper utfordringer for de ansatte, ved at det er vanskelig å knytte lærestoffet til reelle situasjoner som kan oppstå i bedriften.

> *«Men der tror jeg det er forskjell, hvis du sender ut sånne generelle e-lærings leksjoner bare med generell tekst, som er helt korrekt men som er litt for generell og ikke treffer deg der du sitter og jobber, din virksomhet, eller henviser til reglene du skal forholde deg til, da tror jeg effekten er ganske liten. For det er så mye informasjon den enkelte skal forholde seg til i hverdagen allikevel, at hvis det ikke treffer spot-on og ikke rører ved noe personlig ansvar eller følelser, da tror jeg ikke at det har noen effekt»* - Informant 1

Når man diskuterer effektiviteten av slike sikkerhetsbevissthets program og opplæring, kan det se ut som om dette også er en faktor det bør tas hensyn til. Dette kan stille spørsmål til om alle de ferdigpakkene som utarbeides av eksterne aktører blir for generelle til at det skal oppnå best mulig effekt.

Det ble ikke gjennomført noen evaluering av e-læringskursene spesifikt, men det ble lagt ut en spørreundersøkelsene hvor det ble kartlagt om hvorvidt de ansatte ønsker å lære om informasjonssikkerhet. Dersom det foreligger et ønske om å lære, kan dette også være en indikator på at man forstår alvorlighetsgraden av informasjonssikkerhet, og hvorfor dette er viktig. Videre bekreftes det at begge informantene har observert endringer i de ansattes atferd og bevissthetsnivå når det kommer til informasjonssikkerhet. Dette er derimot forårsaket av sikkerhetskampanjen som en helhet, da plakater, roll-ups og andre tiltak også er viktige faktorer som skal skape bevissthet. Men ved å se på noen av de ansattes tanker om e-leksjonene ser det ut til å ha spilt en rolle i å øke det generelle bevissthetsnivået. Det har derimot ikke vært mulig å observere om dette har videre påvirkning på atferden til de ansatte, da dette ofte krever observasjoner oer lengre tid.

Et annet viktig punkt som fremkom gjennom begge intervjuene var måten lærestoffet ble kommunisert ut til de ansatte. Da humor var et viktig element, var det også viktig at det ble brukt et forståelig ordforråd.

> *«Det handler litt om å ha de rette folkene til å gjøre det, for det er ikke alle som er like flinke til å ut å kommunisere med folk på deres nivå. Så du må ha de som greier å finne de riktige ordene til å forklare, å ikke komme med pekefingeren men å på en måte være forståelsesfull.»*-Informant1

Dette understøttes også av en av de ansatte, som forteller at «*Det blir fort kjedelig med pekefinger. Jeg er sikker på at man husker det bedre når det er underholdende».* Fra dette utsagnet kan det også tyde på at måten lærestoffet fremlegges, i tillegg til ordforrådet som blir brukt også har en stor effekt på om leksjonen er underholdende eller ikke, og om den evner til å holde på brukernes oppmerksomhet. Humor elementet forsterkes også når det brukes egne ansatte, da spesielt også for de som deltar i videoen, og de som kjenner vedkommende.

Det må også tas hensyn til at det ikke nødvendigvis er alle som vil synes at den samme metoden er like effektiv, og at noen vil lære mer effektivt gjennom andre metoder.

> *«Konklusjonen min er at du aldri greier å treffe alle ansatte med et tiltak. Så du må alltid gjøre flere ting, og så vite hvilke tiltak som fungerer for hvem slik at man alltid har tiltak som treffer alle. Det er ivhertfall konklusjonen fra praksis.»*-Informant1

Gjennom det ene intervjuet hadde Informant2 også noen egne tanker og innspill rundt tema digital læring.

> *«Du kan godt si at digital læring er vel og bra og har sine styrker og svakheter. Men det er klart at digital læring aldri vil bli bra med mindre folk rundt omkring på*

institutter sier at «dette skal vi gjøre sammen, dette må vi diskutere sammen» gi ord på hva betyr det for oss som et felleskap liksom.»

E-læring er fortsatt et tema hvor det foreligger lite faglig grunnlag om hvor effektivt det er. Spesielt i en sikkerhetskampanje og i sikkerhetsopplæring kan det være utfordrende å isolere leksjonenes effekt ut ifra de andre faktorene som er med på å øke bevisstheten til de ansatte. Basert på informantens innspill og erfaringer rundt tema kan det også virke som om effekten av digital læring er avhengig av andre faktorer, da ofte et felleskap av andre ansatte. I det sosiokulturelle perspektivet på læring er utveksling av informasjon, tanker og erfaringer blant mennesker en del av læringsprosessen. I Bedrift A benyttes det i denne sammenheng også digitale verktøy som Yammer, hvor det tilrettelegges for kommunikasjon mellom ansatte. På denne måten åpner man en mulighet til å stille spørsmål og starte diskusjoner rundt informasjonssikkerhet. Dette må også ansees som en faktor som kan bidra til å øke kunnskap og bevissthet rundt tema. Effekten til e-læring vil også være avhengig av hvordan lærestoffet når ut til den enkelte. Følgende sitater fra intervjuet illustrere dette.

I løpet av intervjuet var det også interessant å høre hvilke tanker informantene hadde til effekten av sikkerhetsopplæring og om den kan bidra til å endre de ansattes atferd. I tillegg til om digitalisering av denne prosessen hadde noen innvirkning på tankemåten/bevissthetsnivået eller atferden til de ansatte.

> *«Jeg tror det har en effekt, helt klart. Kanskje ikke på alle, for noen synes bare det er fjas, og vet best selv. Det vil de alltid gjøre på en måte. Men jeg tror du kan endre atferd hos ganske mange, litt hos ganske mange. For du kan lære dem å stille det ene ekstra spørsmålet «skal jeg åpne mailen, skal jeg ikke åpne mailen? Skal jeg spørre noen kanskje før jeg åpner den? Eller skal jeg ikke gjøre det?» Det tror jeg du kan få til. Det er ikke sikkert du kan få til store atferds endringer, men det små, det lille- utvikle den ryggmargsrefleksen om å være litt skeptisk, det tror jeg du kan få til. Men det handler litt om hvordan det legges frem.»* -Informant1

Sikkerhetsopplæring

Det ble rundt dette tema stilt spørsmål om hvilken oppfatning informanten hadde rundt effekten av sikkerhetsopplæringen, og om det er noe som evalueres. Grunntanken bak dette var å undersøke om effekten av sikkerhetsopplæring og bevissthetsprogrammet eventuelt reflekteres i en reduksjon av uønskede hendelser, eller økning i spam epost som rapporteres. Som det ble avdekket gjennom intervjuet vil ikke slike metrikker nødvendigvis gi en korrekt gjenspeiling av hele bildet.

> *«Vi har alltids hatt måling på eposter i spam-filteret, innbruddsforsøk og sånne ting har vi jo tall på, men det sier aldri alt, på en måte. Det går ikke an å si om utviklingen er positiv eller negativ. Det eneste vi vet er at det alltid er ting som skjer som vi ikke vet noe om, og det er kanskje de hendelsene som er de verste, egentlig.»*

Slik at det på dette vis også blir vanskelig å se rollen til e-leksjonene opp i det hele. Gjennom informantens observasjoner ble det fastslått at de fleste ansatte i Bedrift A hadde et greit bevissthetsnivå og forståelse i forhold til de trusler man kan møte på i arbeidshverdagen. I tillegg ble fremhevet at arbeid med informasjonssikkerhet og er et kontinuerlig arbeid noe som fremmes gjennom følgende sitat fra intervjuet

> *«Vi trenger å kjøre kontinuerlig oppmerksomhet, for at jeg trur det at vi greide å gjøre det i flere år på rad, samtidig som vi jobbet og var synlig mellom kampanjemåned, altså kampanjemåneden i seg selv blir fort glemt hvis vi ikke gjør noe imellom. Det er lang tid fra en måned og til 12 måneder frem i tid på en måte. Så det har hatt en kjempeeffekt og det er viktig å holde trøkket oppe, for det gjør at folk føler hele tiden at kanalen er åpen for å spørre om hjelp, og folk hele tiden er litt bevisst.»* - Informant1

Blant de ansatte ble det også nevnt at en repetering av lærestoffet kunne vært nyttig, da det ofte kan bli glemt dersom man ikke bruker informasjonen og lærestoffet i praksis. Slik at kontinuitet er en annen viktig faktor når det kommer til sikkerhetsopplæring. Bedrift A er i tillegg en stor organisasjon, og det var i den grunn også interessant å undersøke om det ble lagt merke til variasjon i bevissthetsnivået på tvers av de ulike instituttene.

> *«Det er ikke så store forskjeller mellom instituttene, men det kan være veldig store forskjeller mellom enkelt medarbeidere. Men det tror jeg er uavhengig av hvor de jobber egentlig. [..] Det er fortsatt veldig mange med teknologisk bakgrunn som aldri har lært informasjonssikkerhet i studiene. Så jeg tror det handler mer om personlig interessene egentlig. Om man leser de sakene som står i media, eller man ikke gjør det, om man skjønner det er relevant for en selv eller ikke, det tror jeg egentlig er uavhengig av hvilken fagbakgrunn man har»*

Blant de ansatte ble det indikert at informasjonssikkerhet var et samtaleemne ofte i tilknytning til hendelser i nyhetsbildet, og på hvilken måte disse hendelsene var aktuelle for Bedrift A og eget ansvarsområdet.

> *«Men det vi ser er at vi har jo greid å plante en bevissthet hos folk. […] det har gått inn som en del av bedriftskulturen. Som betyr at sikkerhetskulturen er ikke så verst. Det er skummelt å si at den er god, for da er det sikkert noe jeg har oversett. Men jeg tror ikke at den er så verst.[…]Jeg tror de aller fleste er ganske bevisst på både hva de kan møte av trusler, og hvordan de skal håndteres og at det er lov til å spørre om hjelp ikke minst. Samtidig så endrer truslene seg hele tiden og det kommer stadig nye typer eposter, nye type henvendelser og det må vi minne dem om. Jeg tror ikke det står så verst til, men vi er nødt til å holde trøkket oppe. Jeg håper hvis du spør den jevne ansatt at det er et bevissthetsnivå der da, så det tror jeg.»*

Basert på spørrerunden hos de ansatte påpekte også to av dem at de ofte spurte kollegaer med mer kjennskap til IT om hjelp, noe som kan tyde på at kommunikasjon blant de ansatte, og det å tørre å spørre andre om hjelp kan være en viktig kilde til å øke bevissthetsnivået. En organisasjonskultur hvor det er akseptabelt og oppfordres til å spørre andre om hjelp kan derfor være en god forutsetning.

Diskusjon og analyse

Digital læring og kunnskap

Basert på beskrivelser av de ansatte og gjennom dybdeintervjuet, er det en tydelig indikator på at leksjonene bidrar til en økt bevissthet og forståelse av sikkerhet.

> *«Jeg tenker at digital læring kan fyre av gårde noen tanker hos folk og gi noen gode refleksjonsspørsmål. Men derfra og ut så er det dialogen og diskusjonen som foregår mellom mennesker rent fysisk som er viktig også. Om det er satt på spissen så kan det jo på en måte skje alle at digital læring kan du sitte foran egen skjerm å se på. Og så er det veldig varierende i hvilken grad du tar innover deg det du har lært. […] Den sammensyingen av digital og fysisk læring, det er da det virkelig sparker som best. For å ikke bli helt digital*» - Informant 2

Khan et.al (2011) utpeker kunnskap som grunnpilaren innenfor sikkerhetsopplæring og bevissthet. I sin forskning var kunnskap en tilstedeværende komponent i den digitale læringsmetoden for sikkerhetsopplæring. Under intervju med de ansatte hadde flere kjennskap til informasjonssikkerhet fra før. Tre av informantene hadde derimot lært mye gjennom å være involvert i sikkerhetsrelatert arbeid. To av informantene nevnte også at de ofte spurte kollegaer med mer IT-kompetanse om hjelp. En av de ansatte påpekte at leksjonene hadde bidratt til en økt forståelse om *hvorfor* visse regler og prosedyrer måtte følges. Noe som ifølge Daler.et al(2010) var et viktig moment for å motivere til sikkerhetstenkning. Det er derimot vanskelig å isolere effekten av leksjonene sammenlignet med andre kilder til kunnskap, men basert på de ansattes besvarelser virker det som alle hadde lært noe nytt fra leksjonene.

Ettersom leksjonene hos Bedrift A var en sammensetning av video og tekstlige forklaringer, er det hensiktsmessig å se nærmere på om videobasert læring kan føre til en mer effektiv anskaffelse av kunnskap. Det er derimot variasjon blant forskning i hvilken grad video-distribuert læring er mer effektivt sammenlignet med standard tekstbaserte metoder. I empiri utført av Torgersen (2012) blir det brukt ulike multimediavirkemidler blant studenter for å sammenligne hvilken metode som gir best læringseffekt. Studien konkluderte med at den tekstbaserte metoden ga best effekt.

«Det trenger ikke nødvendigvis være sånn at de virkemidlene du liker best, gir best læringsutbytte.»(Nordahl & Torgersen, 2012)

Det ble derimot presisert at de ulike multimedia virkemidlene også krever at man tar ulikt hensyn til oppbygging og tilrettelegging av programmene. Dette understøttes også av tidligere forskning som påpeker at bruk av digital læring stiller høyere pedagogiske krav.(Koppang Frøjd, 2018) Dette er derimot forskning mer spesifisert innen høyere utdanning, hvor læringsmålene som regel er mer omfattende. Forskning gjennomført av Kumaguru et.al(2007) har derimot analysert effektiviteten av ulike multimediavirkemidler mer spesifikt innen sikkerhetsopplæring og bevisstgjøring. Det ble i denne studien gjennomført tester mellom video-basert, tekst-basert og gamification-basert distribusjon av læring. Disse testene ble utført med phising som tema, for å se hvilke metoder som

forbedret brukernes evne til å gjenkjenne phising, og hva man skulle unngå dersom de skulle bli utsatt for slike angrep. Studien avslørte at over 50% prefererte en video-basert form for sikkerhetsopplæring, noe som også kan gjenspeiles i de ansattes fortellinger. Resultatene av studien avslørte også at video-basert læring ga mest økning i bevissthetsnivået, i tillegg til at både de tekstbaserte og videobaserte metodene resulterte i et dypere kunnskapsnivå rundt phising-forsøk.

En av de mest merkbare fordelene med digital læring er tilgjengeligheten. Leksjonene ligger alltid tilgjengelig på bedriftens læringsportal, men det var derimot ingen av de ansatte hadde behov for å gå tilbake til leksjonene. Selv påpekte de også at materialet var lett å huske, men en av de ansatte nevnte at en repetisjon av noen emner kunne vært nødvendig. Spesielt ettersom det ikke var alle emner innenfor informasjonssikkerhet som gjenspeilte seg i arbeidet like ofte, og at det derfor kunne bli glemt. Gjennom et av dybdeintervjuene ble det også påpekt at tilgjengelighet er gunstig når det er nyansatte som skal gjennom den samme sikkerhetsopplæringen, og at de på denne måten raskt og effektivt få en innføring i bedrift A sin sikkerhetspolitikk. Kunnskaps element kan på dette viset stå sterkere i digitale læringsmetoder, da det tillater at nyansatte får kunnskap om retningslinjer og rutiner i forhold til sikkerhet mer effektivt, sammenlignet med tradisjonelle læringsmetoder.

Hvor godt de ansatte innlemmer stoffet i sikkerhetsopplæringen kommer an på hvor relevant de oppfatter materialet for seg selv og egen arbeidssituasjon. Leksjoner som føles upersonlig, og for generelle, vil bli filtrert bort.(Wilson & Hash, 2003) Dette understøttes også gjennom følgende sitat fra dybdeintervjuet: *«Men der tror jeg det er forskjell, hvis du sender ut sånne generelle e-lærings leksjoner bare med generell tekst, som er helt korrekt men som er litt for generell og ikke treffer deg der du sitter og jobber, din virksomhet, eller henviser til reglene du skal forholde deg til, da tror jeg effekten er ganske liten.»* -Informant 1

Videre påpeker Wilson & Hash (2003) at opplæring og bevissthetsprogram kan være effektive dersom materialet fremstilles på en måte som er interessant. Digital læring kan på dette området være fordelaktig, da en av de ansatte påpekte at bruk av video gjorde opplæringen mer interessant. Dette forutsetter derimot fremdeles at videoen oppleves som relevant for de ansatte.

Digital læring og holdning

Khan.et al (2011) fant også frem til at digital læring inneholdt den holdnings-endrede delen. Spørsmålene stilt under intervjuet siktet ikke spesifikt etter å kartlegge holdningen de ansatte har til informasjonssikkerhet, men mer nærmere hvilke erfaringer og evalueringer de har til selve sikkerhetsopplæringen. Den kognitive komponenten blir i denne sammenheng vanskelig å definere, da det ikke ble kartlagt hvilke tanker og ideer som eksisterte om sikkerhetsopplæring generelt. Alle ansatte hadde derimot positive følelser, evalueringer og erfaringer tilknyttet leksjonene. Videosnuttene skapte følelser av engasjement ved at det ble benyttet visuelle læringsmetoder og at det ble brukt humor. Videre påpekte også en av de ansatte at det var brukervennlig i den form at de var enkel å gjennomføre, samtidig som de også var forståelig for de uten mye IT-kompetanse.

Spørsmålet blir derimot om det er noen unike egenskaper ved at leksjonene er digitalisert, som gjør at de oppfattes positivt og vekker positive følelser hos de ansatte?

Det første som kan påpekes er at Ansatt 1 beskriver lengden på leksjonene som en fordel, og at dette kan ha en sammenheng med at det også er lett å gjennomføre. Fordelen med NanoLæring gjør at leksjonene også blir veldig «to-the-point», slik også en av informantene velger å beskrive det. Samtidig stiller dette også krav til en kvalitetssikring som forsikrer at leksjonene kommer til poenget, og at de tar med de viktigste temaene. (Marthinsen, 2015)

Manke (2013) konkluderte i sin forskning at kreativitet var et viktig suksesskriterium for å øke de ansattes engasjement i sikkerhetsopplæringen. I denne rapporten var det tatt utgangspunkt i en rekke sikkerhetsprogram hos ulike bedrifter. Resultatet viste at mer kreative tilnærminger til sikkerhetsopplæring hadde en positiv virkning på de ansattes engasjement i sikkerhet. Deltagende aktiviteter som involverte de ansatte hadde også høy effekt. Innenfor digital læring er det eksempelvis scenariobasert og interaktivt innhold som kan representere en slik deltagende aktivitet. Hos Bedrift A sine leksjoner var det de tekstlige forklaringene som inneholdte en grad av interaktivitet, hvor brukere kunne klikke seg videre i eget tempo. Bruk av egne ansatte i videosnutten bidro til å skape engasjement også for de kollegaer som hadde kjennskap til de som deltok i filmsnutten.

Det kan tenkes at dersom sikkerhetsopplæringen greier å skape positive følelser og økt engasjement, kan det atferdsmessige leddet påvirkes ved at opplæringen er noe de har lyst til å gjennomføre neste runde, og at det på denne måten øker deltagelse. Engasjerende og underholdende innhold, i samarbeid med NanoLæring, kan på denne måten være en viktig motivasjonsfaktor for gjennomføring av leksjonene. Dette forteller ikke nødvendigvis noe om hvor sterk holdning de har til informasjonssikkerhet.

Digital læring og atferd

Endring av atferd settes ofte som et mål, da det sier noe om hvilken grad den eksplisitte kunnskapen har blitt internalisert. Med videre utgangspunkt i Khan.et al (2011) sin forskning var det den atferdsmessige delen som manglet i digital læring. Årsaken til at denne var fraværende skyldes at endring i atferd avhenger av intensjonen til individet. Både intensjon og subjektive normer var en fraværende del i digital læring, noe som dermed ikke kunne utløse en endring i atferd. Khan et.al gruppe diskusjoner som ble rangert som den mest effektive metoden. Dette understrekes også i følgende sitat fra det ene dybdeintervjuet:

«men du har mye større mulighet for å kunne løfte kunnskapen/bevisstheten hvis man snakker med andre kollegaer om det samme. For da vil du få dine og mine erfaringer, noen vet litt mer enn andre for eksempel, og har andre erfaringer og spille på.» - Informant 2

Digital læring kan derimot ha den fordelen ved at man gjennom læringsportalen kan holde styring på hvor mange som gjennomfører kursene. Bedrift A arrangerte konkurranse rundt hvilke avdelinger som gjennomførte flest leksjoner, i tillegg til at det ble delt ut diplomer som de ansatte hang opp ved kontordøren. Gjennom læringsportalen kan en oversikt over påmelding og gjennomføring av leksjonene åpne for mulighet til å skape konkurranse rundt sikkerhetsopplæringen. Gjennom begge dybdeintervjuene virket det som om konkurranses hadde positiv effekt, ikke bare i form av deltagelse, men

også i form av at det bidro til å skape motivasjon. Den avdelingen som hadde mest deltagelse fikk premie. På dette viset blir gjennomføring av leksjonene også noe man jobber mot som en del av et felleskap.

Digital læring kn på dette vis legge et bedre utgangspunkt for andre motivasjonstiltak, som konkurranse eller gamification. Slik at digital læring i seg selv ikke nødvendigvis er nok til å endre atferd, men at det kan fungere som en komplementær metode til andre tiltak og aktiviteter innenfor et sikkerhetsprogram.

«Det er ikke sikkert du kan få til store atferds endringer, men det små, det lille- utvikle den ryggmargsrefleksen om å være litt skeptisk, det tror jeg du kan få til. Men det handler litt om hvordan det legges frem.» -Informant1

Oppsummering og konklusjon

Hensikten med denne oppgaven har vært å undersøke problemstillingen «*Hvordan kan digital læring ha en effekt på kunnskap, holdninger og atferd i sikkerhet?*»

Gjennom denne oppgaven har det kommet frem ulike fordeler og aspekter ved e-læring som muligens kan bidra til å påvirke kunnskap, holdning og atferd. De ansatte påpekte selv en økt kunnskap og bevissthet som resultat av leksjonene. Hvordan økning i kunnskapsnivået hos e-læring sammenlignes med de andre tiltakene er derimot uvisst. Tilgjengeligheten til digital læring var derimot en fordel i forhold til nyansatte i bedriften, da det var mulig å få en rask innføring i sikkerhetsregler og prosedyrer hos Bedrift A. Digital læring kunne også ha en påvirkning i forhold til hvor godt kunnskapen innlemmes hos de ansatte.

Innenfor holdninger hadde leksjonene en affektiv påvirkning, ved at det skapte engasjement gjennom bruk av humor og egne ansatte som skuespillere i videosnutten. Dette kunne videre påvirke det atferdsmessige leddet ved at leksjonene var noe man hadde lyst til å gjennomføre neste runde. De ansatte hadde en positiv holdning til leksjonene, men hvordan holdningen til sikkerhetsopplæring kan påvirke holdning til informasjonssikkerhet var vanskelig å kartlegge i denne studien. Dette kan derimot undersøkes gjennom videre forskning.

Det var ingen konkret indikator på at digitalisering av læring kan påvirke atferd gjennom de ansattes besvarelser. Men heller at e-læring, i samarbeid med en læringsportal, kunne tilrettelegge for tiltak som kunne skape engasjement og motivere til gjennomføring av sikkerhetsopplæringen. Det kan med dette konkluderes at digital læring kunne bidra til en kunnskapsmessig påvirkning ved å bruke videobasert metode, som gjorde sikkerhetsopplæringen mer interessant og vekket oppmerksomhet.

Kildeliste

Arkorful, V., & Abaidoo, N. (2014). *The role of e-learning, the advantages and disadvantages of its adoption in Higher Education. 2*(12), 14.

Busch, T. (2013). *Akademisk Skriving*. Fagbokforlaget.

Daler, T., Gulbrandsen, R., Høie, T., & Sjølstad, T. (2010). *Håndbok i datasikkerhet*. Fagbokforlaget.

E. Derouin, R., Fritzsche, B., & Salas, E. (2005). E-Learning in Organizations. *Journal of Management - J MANAGE*, *31*, 920–940. https://doi.org/10.1177/0149206305279815

Engvig, M. (2010). *E-læring*. Tapir Akademisk Forlag.

Epignosis. (2014). *e-learning Concepts, Trends, Applications*. 110.

Garder B. Gjertsen, E., Gjære, E. A., Bartnes, M., & Rocha Flores, W. (2017, januar 1). *Gamification of Information Security Awareness and Training*. 59–70. https://doi.org/10.5220/0006128500590070

Ghirardini, B., Food and Agriculture Organization of the United Nations, Germany, & Bundesministerium für Ernährung, L. und V. (2011). *E-learning methodologies: a guide for designing and developing e-learning courses*. Hentet fra http://www.fao.org/docrep/015/i2516e/i2516e.pdf

Hjertø, G., & Klefstad, B. (2018). L11 Kulturprogrammet – IBED2003 Informasjonssikkerhet og... Hentet 18. mai 2019, fra https://ntnu.blackboard.com/webapps/blackboard/execute/content/file?cmd=view&content_id=_107301_1&course_id=_3126_1

Jacobsen, D. I., & Thorsvik, J. (2016). *Hvordan organisasjoner fungerer* (4th utg.). Fagbokforlaget.

Khan, B., Alghathbar, K., Irfan Nabi, S., & Khan, K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African journal of business management*, *5*. https://doi.org/10.5897/AJBM11.067

Koppang Frøjd, E. (2018, august 6). – God digital undervisning krever bedre pedagogikk. Hentet 19. mai 2019, fra https://forskning.no/partner-oslomet-skole-og-utdanning/god-digital-undervisning-krever-bedre-pedagogikk/1216418

Kvalnes, P.-H. E. (2016). *Utfordringer med e-læring for heterogene organisasjoner*. 153.

Leseth, A., & Tellmann, S. (2018). *Hvordan lese kvalitativ forskning?* Cappelen Damm.

Mannion, S. (2007). *Research methodology series Interviewing in qualitative research: The one-to-one interview*. Hentet fra https://www.academia.edu/6166493/Research_methodology_series_Interviewing_in_qualitative_research_The_one-to-one_interview

Marthinsen, H. (2015). *Nanolæring «opplæring i små porsjoner»*. 15.

Mathisen, J. (2004). *Measuring Information Security Awareness – A survey showing the Norwegian way to do it*. 102.

McLeod, S. A. (2018). Attitudes and Behavior | Simply Psychology. Hentet 19. mai 2019, fra https://www.simplypsychology.org/attitudes.html

Nordahl, M., & Torgersen, G. (2012). Lærte oftest best med tekst. Hentet 19. mai 2019, fra https://forskning.no/psykologi-skole-og-utdanning-pedagogiske-fag/laerte-oftest-best-med-tekst/719680

Omer Habeeb, A. (2015, september 21). Is Bite Sized Learning The Future Of eLearning? Hentet 18. mai 2019, fra eLearning Industry website: https://elearningindustry.com/bite-sized-learning-future-of-elearning

Schrader, P. G., & Lawless, K. (2004). The knowledge, attitudes, & behaviors approach how to evaluate performance and learning in complex environments. *Performance Improvement*, *43*, 8–15. https://doi.org/10.1002/pfi.4140430905

Schreurs, J., Ehler, U., & Moreau, R. (2008). *Measuring e-learning readiness*. 8.

Sian KOH, N., Gottipati, S., & Shankararaman, V. (2018, juni 20). *EFFECTIVENESS OF BITE-SIZED LECTURE ON STUDENT LEARNING OUTCOMES*. https://doi.org/10.4995/HEAD18.2018.8027

Trang. (2018, mars 6). Microlearning: Features, Benefits, and Drawbacks - ActivePresenter. Hentet 19. mai 2019, fra Atomi Systems, Inc. website: https://atomisystems.com/elearning/microlearning-features-benefits-drawbacks/

Wilson, M., & Hash, J. (2003). *Building an Information Technology Security Awareness and Training Program* (Nr. NIST SP 800-50; s. NIST SP 800-50). https://doi.org/10.6028/NIST.SP.800-50

Youssef, Y. (2015). *GAMIFICATION IN E LEARNING*. https://doi.org/10.13140/RG.2.1.4613.4162