Skema A1: Ansøgning om resultatkontraktmidler 2017-18 (aktivitetsplan)

. Font: Times New Roman 11, maks. længde: i alt 10 sider. Der må ikke ændres på spaltebredden.

Aktivitetsplan (titel):	**Kursus: Cybersikkerhed og social engineering**	**Aktivitetsplan nr.:**	
Resumé	Regeringens Nationale Strategi for Cyber- og Informationssikkerhed fokuserer på konsekvenserne ved cyberangreb både for ministerier og kommunale instanser, men også for dansk erhvervsliv[1]. De to største problemområder er cyberspionage og cyberkriminalitet. Her er det Center for Cybersikkerheds (CFCS) trusselsvurderingsenheds afgørelse, at truslen er meget høj[2]. På trods af denne trussel udbydes der meget få kurser i cybersikkerhed i Danmark på nuværende tidspunkt[3]. Det er derfor anbefalingen til regeringen, at der bør udbydes flere kurser og uddannelser inden for cybersikkerhed[3]. Dansk Brand- og sikringsteknisk Institut (DBI) vil i samarbejde med Københavns Erhvervsakademi (KEA) udarbejde et valgfag, som går på tværs af KEAs digitale programlinjer samt et CFPA[4] godkendt kursus for små- og mellemstore virksomheder (SMV). Kurserne tager afsæt i den brede faglige viden, som begge parter besidder, og en stor del af kurserne vil derfor bestå i at videndele og formidle projekt- og forskningsresultater. Projektets formål er at videreudvikle og understøtte de faglige kompetencer inden for cybersikkerhed i Danmark.		
1) Relation til national strategi på området	Dansk erhverv digitaliseres i større grad, hvilket skaber en række nye sikkerhedsrisici. Myndigheder og private virksomheder er afhængige af internettet, hvilket gør dem sårbare overfor cyberspionage, -aktivisme, -terror og -kriminalitet[2]. Antallet af cybertrusler er stigende, og det er derfor vigtigt, at Danmark holder sig orienteret om sikkerhedstrusler, og hvordan myndigheder og virksomheder kan bekæmpe dem. Ifølge CFCS er de to største problemområder inden for cybersikkerhed relateret til cyberspionage og cyberkriminalitet[2]. De kriminelle gør brug af let tilgængelig teknologi til at afpresse eller videresælge personfølsomme data. De kriminelle får i stigende grad adgang til virksomheders systemer gennem manipulationen af medarbejdere også kaldet social engineering. Der er i Danmark behov for at styrke cybersikkerheden for danske SMV'er[1]. Cyberangreb kan være skæbnesvangre for små og mellemstore virksomheder. Det skal derfor sikres, at SMV'erne udnytter de eksisterende muligheder på sikkerhedsområdet[1]. CFCS' trusselsvurderingsenhed anbefaler, at cybersikkerheden styrkes ved at ansætte personer med kompetencer inden for cybersikkerhed, før man udsættes for et cyberangreb[2]. Regeringen ønsker at kortlægge de eksisterende nationale og internationale kurser og uddannelser inden for cybersikkerhed[1]. Dette skal give et mere præcist billede af, hvor der skal gribes ind, når den Nationale Strategi for Cyber- og Informationssikkerhed skal revideres i 2016[5]. Denne kortlægning viser vigtigheden af at have fokus på området.		

[1] Regeringen (2014) National Strategi for Cyber-og Informationssikkerhed – øget professionalisering og mere viden.
[2] Center for Cybersikkerhed (2016) Trusselsvurdering: Cybertruslen mod Danmark.
[3] Deloitte (2015) Kortlægning af viden- og uddannelsesaktiviteter inden for cyber- og informations-sikkerhed på danske uddannelses- og forskningsinstitutioner.
[4] CFPA – Europa. CFPA (The Confederation of Fire Protection Association Europe) er en sammenslutning af brand- og sikringsinstitutter i Europa. Her sættes bl.a. standarder for kurser på tværs af Europa.
[5] Digitaliseringsstyrelsen (2016) National strategi for cyber- og informationssikkerhed.

	Danmark har mangel på IT-kyndige, hvor især kompetencer inden for softwareudvikling og forretningsforståelse er efterspurgte på arbejdsmarkedet. Dette til trods for at der i Danmark er uddannet 80 % flere inden for IT fra 2004 til 2012. Alligevel forventes der, i 2020 en efterspørgselsstigning på 23,9 % for IT-uddannede[6]. Allerede nu betyder det, at tre ud af 10 virksomheder i dag ikke kan få IT-stillinger besat og mange må derfor opgive jagten[7]. Det anbefales, at der udbydes flere kurser og uddannelser inden for cybersikkerhed, der formidler viden på feltet, men også tillader studerende at specialisere sig inden for bestemte fagområder inden for cybersikkerhed[3]. Dette er vigtigt for at sikre det danske erhvervslivs konkurrenceevne på det internationale marked[2].
2) Målgruppe og behov	Den primære målgruppe er studerende inden for det digitale programområde hos KEA. Den sekundære målgruppe er SMV'er, der ønsker at beskytte deres virksomhed imod cyberangreb. Der findes i dag 106 kurser i Danmark, med cybersikkerhed som en del af kursusmaterialet. Det er overvejende universiteterne der udbyder kurserne. Hoveddelen af erhvervsakademierne underviser ikke deres elever inden for feltet og mangler dermed en holistisk tilgang til cybersikkerhed. KEA udbyder med fire kurser flest i cybersikkerhed[3]. I Danmark findes der 75 certificeringskurser inden for cybersikkerhed. Certificeringskurser bruges i dag som efteruddannelse for beskæftigede professionelle til at holde sig opdateret med seneste viden inden for faget. Certificeringer giver et bevis for specifikke, praktiske evner og handler om konkrete problematikker, som deltagerne kan møde i deres virksomheder i hverdagen. Selvom der er stor forskel på niveau og varighed fra certificering til kurser, har det danske erhvervsliv brug for begge uddannelsesmuligheder[3]. Mangel på ressourcer og opbakning udgør de største barrierer for at sætte fokus på cybersikkerhed for uddannelsesinstitutionerne i forhold til at starte nye uddannelser. Derudover er der ganske få undervisere inden for feltet, hvilket kan have alvorlige konsekvenser for skolens forskningsområde og kursusudbud, hvis en underviser går på pension eller skifter job[3].
3) Den nye teknologiske serviceydelse	Projektets formål er at styrke de faglige kompetencer inden for cybersikkerhed. DBI vil i samarbejde med KEA udvikle kurser i cybersikkerhed. Indholdet skal spænde fra de menneskelige faktorer i Social Engineering, til fysisk sikkerhed med elektronisk overvågning, lås og alarmer på døre. Kurserne skal gå på tværs af udvalgte uddannelser hos KEA inden for det digitale programområde og vil spænde fra akademi- til bachelorniveau. Kursernes indhold udvikles af KEA, mens DBI tilfører faglig dybde og kontakt til erhvervslivet. Kursusindholdet vil omhandle den nyeste viden inden for området samt resultater og events fra DBI's sikkerhedsafdeling og deres forskningsprojekter. KEA sikrer det læringsmæssige udbytte af kurserne samt inkorporerer kurserne i deres normale undervisningsforløb. Kursernes form og indhold vil løbende blive justeret til uddannelsen og tilpasset de studerendes tekniske niveau. Kursusformen inkluderer derfor både klassiske kurser, webinarer, e-learning og gamification.

[6] IT-Branchen og Dansk Erhverv (2015) It-branchen i den internationale konkurrence: styrker og svagheder.
[7] Højbjerre Brauer Schultz, Kubix og Alexandra Instituttet (2016) Virksomheders behov for digitale kompetencer.

	DBI vil med støtte fra KEA, udvikle et CFPA godkendt kursus, der skal udbydes bredt og eventuelt kan bruges som overbygning til eksamineret sikringsledere (ESL). Kurset skal efteruddanne beskæftigede inden for sikkerheds- og IT-branchen rettet mod SMV'er. SMV'er er særlig sårbare overfor cyberangreb, hvor specielt videndeling og awarenesstræning i sikker cyberadfærd kan skabe øget bevidsthed om IT-sikkerhed. CFPA Europe er en sammenslutning af nationale brand- og sikkerhedsinstitutter i Europa[8]. Organisationens mål er at danne fælles standarder for kurser og undervisning i hele Europa. CNPP (Fransk nationalt brand- og sikkerhedsinstitut) har her søgt om at oprette en standard for cybersikkerhedskurser, omhandlende social engineering, spyware, malware, m.m. Bliver dette kursus vedtaget som en CFPA-standard, vil det blive udgangspunktet for et kommende DBI-kursus i cybersikkerhed.
4) Aktiviteter	Projektet består af tre arbejdspakker: Arbejdspakke 1 – Styrkelse af valgfag i cybersikkerhed hos KEA: *Kursusudvikling hos KEA. Der udvikles en kursusbeskrivelse og herefter gennemføres et pilot kursus, der evalueres før det færdige kursusforløb gennemføres. KEA gennemfører kurset, hvor DBI bidrager til indhold og enkelte undervisningsgange.* Arbejdspakke 2 – Udvikling af CFPA kursus: *DBI udvikler CFPA godkendt-kursus med udgangspunkt i CNPPs oplæg. Kursusbeskrivelsen udarbejdes i samarbejde med KEA, hvorefter der udføres et pilotkursus. Ud fra evalueringen af dette gennemføres et helt kursusforløb hos DBI, hvor KEA bidrager til indhold og enkelte undervisningsgange.* Arbejdspakke 3 – Formidling: *DBI og KEA formidler projektet ved at gøre brug af relevante nyhedsplatforme. Der har i den seneste tids medier været stor fokus på privacy og cybersikkerhed ligesom emnet behandles i diverse aktuelle TV-serier og dokumentarer*[9]. *Efter projektets afslutning vil DBI udgive en artikel i fagbladet 'Brand og sikring', der både omhandler valgfaget på KEA og DBI's CFPA. De studerende på KEA vil løbende sætte fokus på området gennem nye medier som fortællinger via Facebook, sociale eksperimenter via YouTube, skabe et hashtag på Twitter m.m.*
5) Vidensamarbejde og -hjemtagning	Både DBI og KEA forpligter sig til at dele viden og ressourcer gennem projektet. Dette indbefatter, men er ikke begrænset til: • Undervisningstimer og -materiale • Projektresultater • Tekniske faciliteter Forud for projektet har DBI arbejdet med flere projekter inden for cybersikkerhedsområdet. Mange af disse projekter har fokus på vidensprednin og der lægges især fokus på, hvordan man skal formidle den viden, som projektet skaber. Dette projekt kan derfor betragtes som en yderligere formidling af resultater fra tidligere forskningsprojekter og viden på området.
6) Inddragelse og vidensprednin	DBI har mere end 10.000 kursister årligt og tilbyder en lang række kurser indenfor brandteknik og sikring, som strækker sig fra korte AMU kurser til længere kompetencegivende uddannelser. Derudover er DBI specialister i virksomhedsefterforskning med særligt fokus på digitalt angreb- og ansvarsundervisning inden for områder

[8] CFPA (2013) CFPA EUROPE.
[9] DR (2015) Tema: du bliver overvåget.

	som for eksempel pharma og elektronik. DBI samarbejder med forskellige partnere på disse to forskningsprojekter inden for social engineering (SE). - SAVE-projektet søger at undersøge og skabe opmærksomhed omkring SE problemet blandt danske og internationale virksomheder. - DOGANA- projektets formål er dels at definere organisationers sårbarhed over for SE og at reducere de forbundne risici. Dette indebærer strategitræning i en virksomhed, hvor medarbejderne trænes i forskellige SE-situationer og lærer, hvordan de skal reagere på truslerne. Innovationsnetværket for Produktion (Inno-Pro) har udarbejdet en ansøgning om en national platform for cybersikkerhed. Dette sker i samarbejde med Innovationsnetværk for it (InfinIT), Innovationsnetværket for Finans IT (IFFI), Copenhagen Fintech Innovation and Research (CFIR), Alexandra instituttet, Delta og DBI. Denne ansøgning er et eksempel på DBI's samarbejdsprojekter med institutter, innovationsnetværk og virksomheder om cybersikkerhed. KEA udvikler og udbyder praksisrettede videregående uddannelser på erhvervsakademiniveau og professionsbachelorniveau. Dette sker i nært samarbejde med erhvervsliv og uddannelsesinstitutioner i ind- og udland. KEA fungerer desuden som videncenter for offentlige og private virksomheder. KEA har over 9.000 studerende, hvoraf ca. 3.000 er inden for det digitale programområde[10].
7) Sammenhæng med institutstrategi	DBI er Danmarks førende videncenter for brandsikkerhed og sikring. DBI sikrer liv og værdier ved at levere brand- og sikringsydelser til danske og udenlandske virksomheder. Med digitaliseringen af dansk erhverv er mange værdier i dag blevet immaterielle. Værdi er ikke længere penge i kassen, men også information i cyberspace. Dette betyder at DBI må tilpasse og forny de sikringsløsninger som tilbydes. Nye typer af værdier skal derfor sikres på nye måder. SE handler om det menneskelige aspekt, og hvordan medarbejdere kan manipuleres til at give hackeren den fornødne adgang til systemet[11]. Denne type sikkerhedsbrud kan koste virksomheden flere millioner kroner, og det er derfor vigtigt at uddanne og ansætte personel på området[12]. SE er et af DBI's fokusområder, da både små og store virksomheder er sårbare over for denne type angreb, da man ikke i dag har ordentlige modforanstaltninger til rådighed.
8) Milepæle år 1	• MP 2.1: DBI har udviklet et kursus koncept og har modtaget tilkendegivelser fra interesserede SMV'er • MP 3.2: KEA's studerende har i projektets første år udarbejdet og publiceret mindst 5 videoer med sociale eksperimenter i forhold til cybersikkerhed på forskellige sociale medier. • MP 3.1: Der udarbejdet og publiceret en faglig artikel om projektets resultater til mindst 1 relevant dansk branchetidsskrift eller nyhedsmedie.
9) Milepæle år 2	• MP 1.1: KEA har udviklet, gennemført og evalueret et nyt kursus i cybersikkerhed for KEAs studerende. • MP 2.2: DBI har udviklet, gennemført og evalueret et nyt CFPA-godkendt kursus i cybersikkerhed rettet mod danske SMV'ere.

[10] KEA (2016) OM KEA.
[11] Kaspersky (nda) Social Engineering – Definition.
[12] PwC, Infosecurity Europe and Reed Exhibitions (2015) 2015 Information security breaches survey.