Executive course:

Cybersecurity for Board Members, Executives and Managers

Strategisk og operationel cybersecurity for ledere

"Cybertrusler er en af de største forretningsrisici, vi ser ind i. Derfor er det afgørende, at vores ledere bliver klædt på til at forstå og vurdere trusselsbilledet - og integrere cybersikkerhed i virksomhedernes overordnede strategi."

Nadeem Farooq, underdirektør,
Finanssektorens Arbejdsgiverforening

FA FINANSSEKTORENS ARBEJDSGIVERFORENING

Forord

Når du leder og driver virksomhed i et af de mest digitaliserede samfund i verden, er cybersikkerhed en obligatorisk del af virksomhedens risk-management. Ledelsen har det overordnede ansvar for at beskytte virksomhedens aktiver, og den opgave kræver et tæt samarbejde med de it-sikkerheds-ansvarlige.

Danmarks Tekniske Universitet (DTU) har med Finanssektorens Arbejdsgiverforening (FA) som business partner samarbejdet om en indsats, der adresserer stigende efterspørgsel på kompetencer inden for cyber- og informationssikkerhed gennem fortsat udvikling af efteruddannelse.

Indsatsen har haft til formål

- at afdække kompetencebehov som forudsætning for at kunne skræddersy relevante kompetenceløft rettet mod Bord Members, Executives og Managers.
- At udvikle og gennemføre effektiv, high level kompetenceløft på baggrund af behovsafdækning og et tekninsk afsæt i viden og erfaring fra DTU, Cybersecurity Engineering,

DTU og FA er glade for at kunne præsentere resultatet, som er blevet til et kompetenceprogram bestående af to moduler 'Cybersecurity Essentials' og 'Cyber-risk Management', der hver for sig eller sammen styrker sprog og indsigt til at gribe ansvaret for virksomhedens aktiviteter - proaktivt og velinformeret.

Cybersikkerhed er ledelsens bord

Kritisk punkt på tidens dagsorden

Hvor står jeres virksomhed, hvis et cyberangreb lammer jeres digitale systemer?

I dag er cyberangreb blandt de mest kritiske forretningsrisici, virksomheder står overfor. Et cyberangreb kan skade både indtjeningen, kunderelationer og virksomhedens omdømme.

Derfor rykker cybersecurity stadig højere op på dagsordenen. Ikke kun hos de sikkerhedsansvarlige, men også - og det er helt afgørende - hos bestyrelser og direktioner.

Spørgsmålet er, hvordan du som leder bliver i stand til at træffe balancerede beslutninger, der flugter med virksomhedens interesser og strategi.

Byg bro mellem cyber og business

En stor del af den daglige håndtering af cyberrisiko ligger naturligt nok hos de it-sikkerhedsansvarlige. Risikostyring er imidlertid kernen i enhver forretnings-beslutning, og derfor kræver cyber-risk management også ledelsens stillingtagen.

Desværre viser World Economic Forums rapport 'Global Cybersecurity Outlook 2023', at forståelsen mellem cyber leaders og business leaders stadig lader en del tilbage at ønske. For hvordan skal man som leder prioritere indsatser og ressourcer, hvis man ikke har indsigt i mulighederne - og konsekvenserne?

Det er den kløft, som modulerne Cybersecurity Essentials og Cyber-risk Management er designet til at bygge bro over. Fagligt såvel som sprogligt.

Gør en forskel gennem kulturen

I de fleste virksomheders praktiske hverdag er det svage led faktisk ikke teknologi, men kultur: Ledere og medarbejdere kender ikke forskel på de mange typer cybertrusler - eller alvoren af dem set i deres aktuelle kontekst. Det giver de cyberkriminelle alt for let spil, og derfor fokuserer dette program (især modul 1, Cybersecurity Essentials) også på den menneskelige faktor: Hvordan man skaber en kultur, hvor sikre vaner er en del af brugernes daglige færden.

Ledelsen har brug for cybereksperter for at:

- Beskytte aktiver, forretningsprocesser og kunder.
- Generere vækst og udnytte forretnings-mulighederne i en digitaliseret kontekst.
- Fastlægge virksomhedens risikoprofil og investeringsvillighed.
- Leve op til direktionens ansvar.

Fleksibelt kursus i to moduler

Cybersecurity for Bord Members, Executives, and Managers består af to moduler, du enten kan tage samlet eller hver for sig - alt efter dit behov. Undervisningen foregår på engelsk.

Modul 1: Cybersecurity Essentials
Når ledelsen skal diskutere cybersikkerhed på et kvalificeret grundlag, kræver det et sprog og en teknisk forståelse, der både kan nå og udfordre de ansvarlige for cybersikkerhed i virksomheden.

Derfor fokuserer Modul 1 på at etablere en grundlæggende indsigt i feltet:

- Introduction and Security Trends. Herunder cybersikkerhed, typiske trusler og angrebsveje og forskellige tilgange til cybersikkerhed.
- General Security Concepts. Herunder grundlæggende begreber, forskellige aspekter af cybersikkerhed og principper for den.
- The Role of People in Security (Social Engineering). Herunder potentiel risikoadfærd, sikre vaner samt indsatser for at opbygge en sund sikkerhedskultur.
- Types of Attacks and Malwares. Herunder også fokus på symptomer og relevante forsvar og guidelines.
- Identification and Authentication. Herunder adgangskoders rolle samt hvordan de kan angribes og forstærkes.

Professor Nicola Dragoni
PhD, Deputy Director, Professor in Secure Pervasive Computing, Head of Section Cybersecurity Engineering, Head of DIGISEC - DTU Center for Digital Security

Modul 2: Cyber-risk Management
I en forbundet verden er 100 % cybersikkerhed både umuligt og uvurderligt. Så hvilken indsats skal virksomheden prioritere – og hvor er balancen mellem risici på den ene side og prisen på sikkerhed på den anden side?

I modul 2 skabes der koblingen mellem forretning og cybersikkerhed, og der gåes i dybden med områder som:

- Den konceptuelle ramme. En struktureret tilgang til cyberrisikostyring.
- Konteksten. De faktorer virksomheden skal tage højde for og inddrage i sit arbejde med cyberrisikostyring.
- Vurdering af trusselsscenarier og risici. Hvordan man går videre og dirigerer for at få mest muligt ud af tilgængelige ressourcer.
- Afbalanceret beslutningstagning giver relevante resultater. Muligheder for behandling og kontrol.
- Kommunikation for at kunne informere og engagere relevante parter.

Professor Ketil Stølen
Ph.d. i datalogi, projektleder, foredragsholder, skribent og rådgiver

Du bliver ikke teknisk ekspert. Du bliver i stand til at træffe velinformerede beslutninger.

Vælg det forløb, der passer til dit behov

Du kan tage de to kursusmoduler enten hver for sig eller sammen. Her får du vores anbefaling.

Din rolle	Anbefaling
Leder uden cybersecurity baggrund	Modul 1: Cybersecurity Essentials
Cybersecurity medarbejder inklusiv ledere og bestyrelsesmedlemmer med ekspertise svarende til Modul 1	Modul 2: Cyber-risk Management
Leder eller bestyrelsesmedlem uden cybersecurity ekspertise med behov for indsigt i cybersecurity management	Modul 1: Cybersecurity Essentials efterfulgt af Modul 2: Cyber-risk Management

Modul 1: Cybersecurity Essentials sætter dig i stand til at:

Forstå og vær opmærksom på de mest almindelige cybertrusler.

- Få viden, færdigheder og mindset om cybersikkerhed
- Forstå det skiftende landskab for cybertrusler.
- Etabler en kultur af modstandsdygtighed og forstærk langsigtet succes

Modul 2: Cyber-risk Management sætter dig i stand til at:

Aligne cybersikkerhed med forretningsmål.

- Integrer cybersikkerhedsovervejelser i forretningsplanlægning, beslutningsprocesser og risikostyringsrammer.
- Udvikle informerede strategier.
- Sikre, cybersikkerhed bliver en iboende del af organisationens overordnede strategi.

Hvilke trusler ser du ind i?

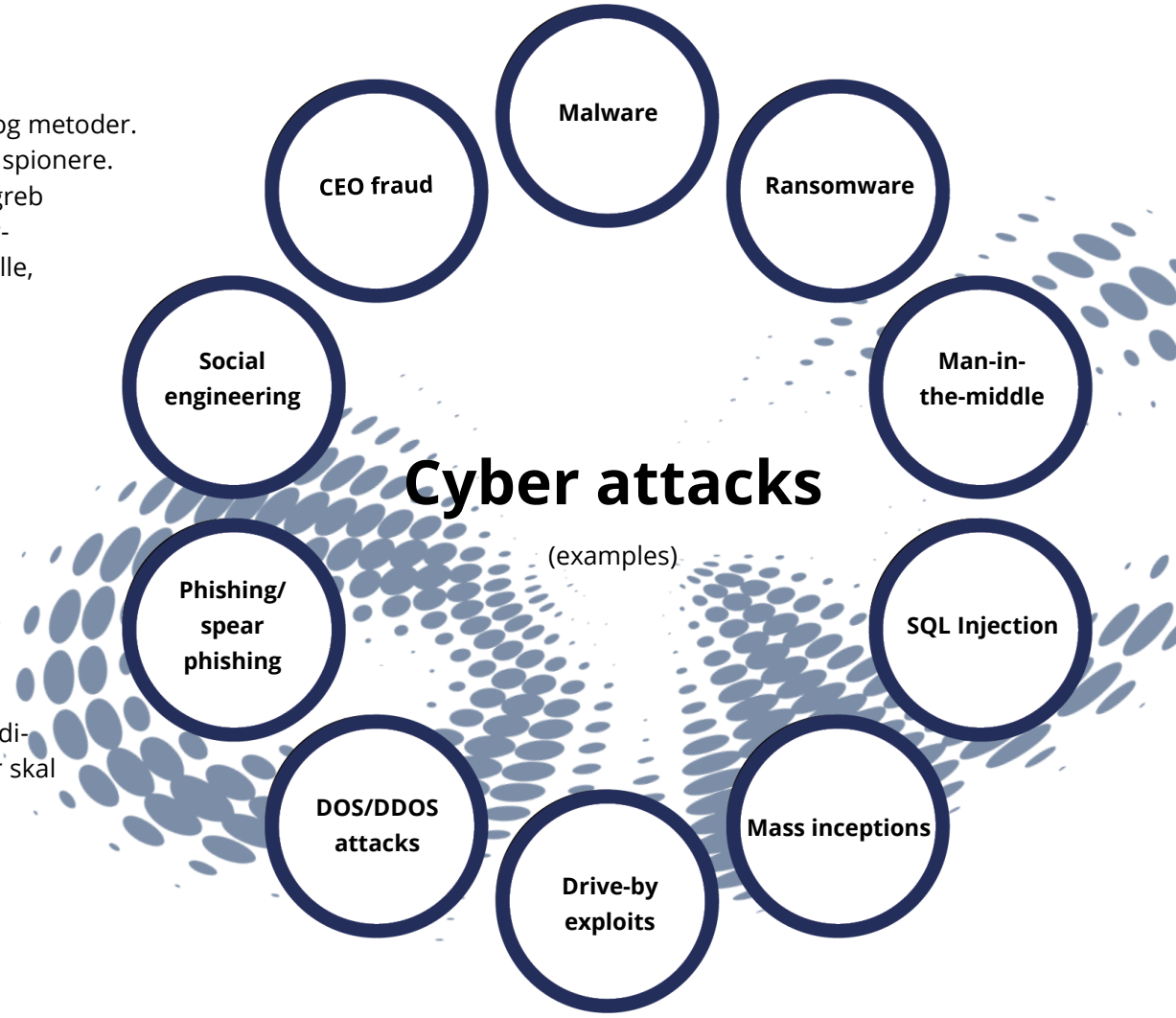
Begrebet cyber-trusler dækker en lang række forskellige angreb med forskellige formål. For at arbejde med en strategi for cybersikkerhed har du brug for indsigt til at vurdere, hvad der er særlig sårbart for netop din virksomhed og diskutere, hvilke indsatser der derfor skal prioriteres.

Det komplekse landskab
Cyberangreb drives af forskellige hensigter og metoder. Nogle angreb sigter mod at stjæle data eller spionere. Andre sigter mod at stjæle penge. Nogle angreb er simple, mens andre er avancerede. Cyber-angreb kan udføres af organiserede kriminelle, suveræne stater, amatører, interne medarbejdere og konkurrenter.

Et vellykket angreb kan i sidste ende lamme virksomheden. Derfor er det afgørende, at du er i stand til at vurdere jeres sårbarhed - og prioritere ressourcerne til de rette modtræk.

De mest udbredte cybertrusler i dag er phishing-e-mails og CEO fraud. Men din virksomheds risikoeksponering afhænger både af branchen, virksomhedens mest værdi-fulde aktiver og dens sårbarheder, og derfor skal den vurderes individuelt.

Det skønnes, at 9 ud af 10 virksomheder allerede er blevet hacket.



Brobygning mellem business og cyber

På den ene side står ledelsen med ansvaret for risiko-styring - og ved, at cyber-truslerne er alvorlige for forretningen. På den anden side står specialisterne i it-sikkerhed, der kender de teknologiske greb. Cybersikkerhedsstrategien er den nødvendige bro mellem de to aktører.

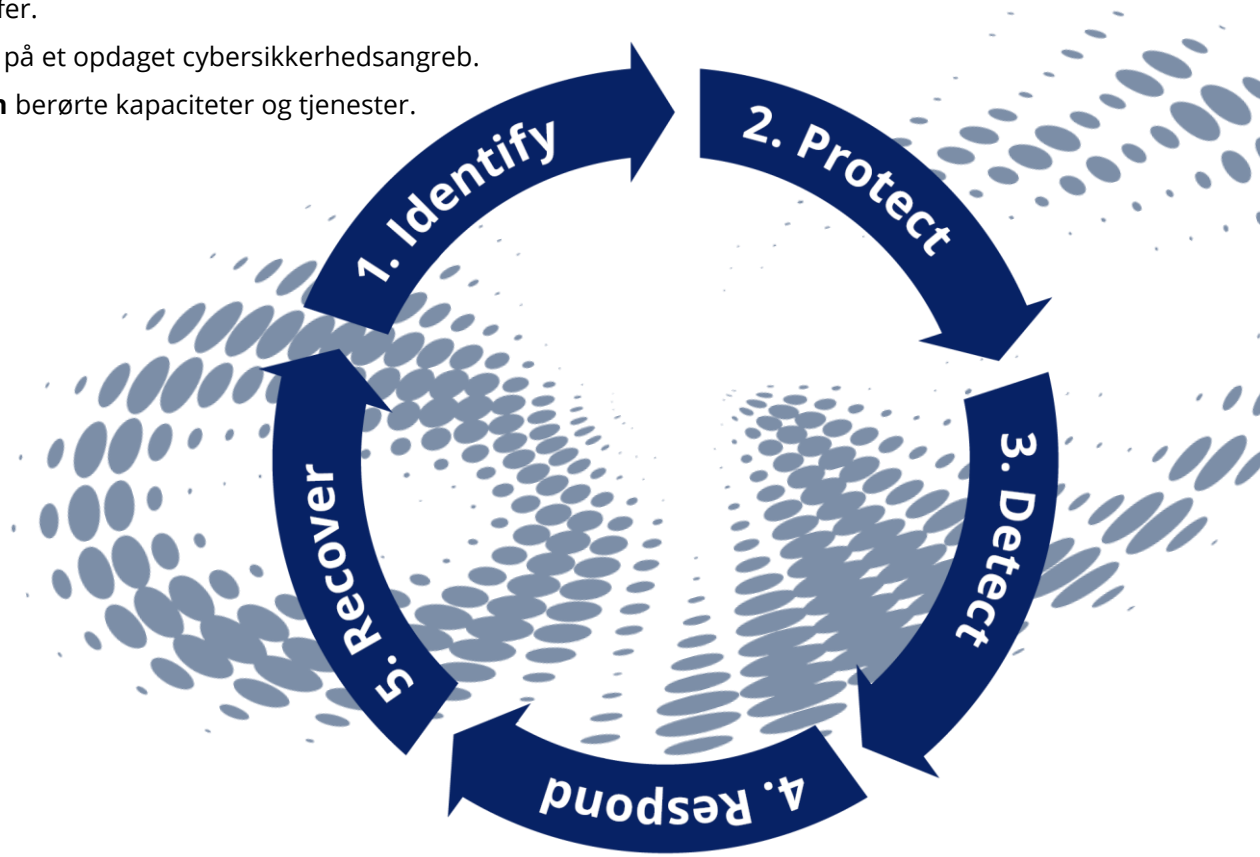
Strategien sætter rammen
Cybersikkerhedsstrategien er den ramme, der sikrer, at alle aspekter af sikkerheden indgår i virksomhedens løbende cyber-risk management. Strategien kan sætte virksomheden i stand til at implementere de fem grundlæggende funktioner i en cybersikkerhedsramme: Evnen til at identificere, beskytte, opdage og reagere på cyberhændelser - samt evnen til at genoprette berørte systemer og aktiver.

Strategien adresserer samtidig alle aspekter af sikkerheden - fra styring og ledelse til værktøjer, processer, mennesker og it. Derfor bør den naturligt stå højt på enhver ledelses dagsorden.

Transformer viden til cybersikker business
Med modulerne Cybersecurity Essentials og Cyber-risk Management er Bord Members, Executives og Managers godt rustet til at træffe beslutninger relateret til en cybersikkerhedsstrategi.

Mål for en cybersikkerhedsstrategi

1. **Identificer** aktiver, sårbarheder, trusler mv.
2. **Beskyt** virksomheden med passende foranstaltninger.
3. **Opdag** om eller hvornår en cybersikkerhedsbegivenhed indtræffer.
4. **Reager** på et opdaget cybersikkerhedsangreb.
5. **Gendan** berørte kapaciteter og tjenester.



Fraud case

En velgørenhedsorganisation var først klar over, at der var et angreb, da deres bank kontaktede dem for at spørge om en ændring af en leverandørs bankoplysninger.

Deres CISO forklarede: ”Vi tjekkede økonomichefens e-mail-konto og opdagede, at der var blevet oprettet en regel for at omdirigere enhver e-mail, der indeholder ordene 'betaling', 'faktura', forfaldne bankoplysninger' osv. til Really Simple Syndication (RSS)) feeds mappe. Her ‘opererede’ svindleren på brødteksten i e-mailen og den vedhæftede faktura med falske bankoplysninger. Det var troværdigt, da hoveddelen af e-mailen tydeligvis kom fra en kendt leverandør, da den besvarede spørgsmål, som kun de kunne have kendt. Vi troede på dette tidspunkt, at vi snævert havde undgået at foretage en betaling til en svindlers bankkonto.”

En anden leverandør mailede en uge senere for at finde frem til betaling af en faktura, som organisationen troede, de havde betalt. Ved at kontrollere betalingsoplysningerne opdagede de, at betalingsmodtagerens kontooplysninger var anderledes end dem på fakturaen.

”Når man ser tilbage, havde økonomichefen bemærket, at folk sagde, at de havde sendt hende en e-mail, men at den tog en dag eller to om at komme igennem, men det mente man bare var en forsinkelse i systemet. Dette vil være en alarm med rødt flag fremover.”

Øjeblikkelig handling

- Økonomichefen ringede til banken og gjorde dem opmærksom på svindelen.
- Vi rapporterede til Action Fraud for at få et referencenummer for forbrydelsen
- Vi rapporterede til The Charity Commission som en alvorlig hændelse

Læringer/fremtidige handlinger

- Vi har opdateret vores processer og procedurer
- Vi kontrollerer ugentlig e-mail-kontoen for at sikre, at der ikke er fastsat regler
    - tjek e-mail-listen over "sikre afsendere" for at sikre, at den er autentiskkontrollere placeringen af eventuelle logins til Microsoft 365 for at sikre, at der ikke er aktivitet på kontoen
    - tjek RSS-feed-mappen for useriøse e-mails
    - bankoplysninger for nye og opdaterede leverandører, der skal bekræftes ved et telefonopkald
- Hvis en betaling online og bankoplysningerne ikke stemmer overens, skal du ringe og tjekke med betalingsmodtageren, at oplysningerne er korrekt
- Implementeret multifaktorgodkendelse til at logge på Microsoft 365

Cybersecurity for Bord Members, Executives, and Managers - tilmelding og praktisk

Se yderligere detaljer om kurset på lifelonglearning.dtu.dk

https://lifelonglearning.dtu.dk/en/compute/single-course/cybersecurityessentials/

https://lifelonglearning.dtu.dk/en/compute/course/cyber-risk-management/

.

Cybersecurity Essentials
Start: 22 November 2023
Location: DTU Kgs. Lyngby
Language: English
Price: 12.500 DKK

Reg. deadline: 10 November 2023

Cyber-risk Management
Start: 5 December 2023
Location: DTU Kgs. Lyngby
Language: English
Price: 12.500 DKK

Reg. deadline: 20 November 2023

Kontakt
Har du spørgsmål til kurset, kan du kontakte:

Nicola Dragoni
Professor, Head of Section
DTU Compute
+45 45 25 37 31
ndra@dtu.dk

Camilla Gudrun Poulsen
Senior Officer
DTU Compute
+45 31 26 75 86
cagupo@dtu.dk

DTU

FA FINANSSEKTORENS ARBEJDSGIVERFORENING