



DAG 2 - TIRSDAG



Program

- Adfærd – og hvorfor det spiller en rolle?
- Mål, målgrupper og afrapportering
- Case-arbejde
- Frokost
- Fremlæggelse



For at skabe en stærk cybersikkerhedskultur må vi forstå, hvorfor medarbejdere træffer bestemte valg, og hvordan man kan påvirke disse valg gennem en forståelse af dem det handler om.



Relevante faktorer

- Manglende risikoforståelse
- Manipulation
- Vaner og bekvemmelighed
- Overbelastning af information
- "Det sker ikke for mig" syndrom
- Manglende konsekvenser ved overtrædelse
- Tillid til teknologi




Manglende risikoforståelse

Mennesker har en tendens til at undervurdere risici, især når de ikke umiddelbart kan se konsekvenserne af deres handlinger.

Det er vigtigt at forklare og visualisere potentielle konsekvenser af usikker adfærd.

Eksempler på manglende risikoforståelse:

- En medarbejder downloader en vedhæftet fil fra en ukendt e-mailadresse uden at indse risikoen for malware.
- Brug af usikre Wi-Fi-netværk uden at forstå faren ved potentielt at udsætte følsomme data.



Refleksion: Find et eksempel på hvor manglende risikoforståelse har spillet ind på jeres adfærd?




Social manipulation

Angribere udnytter ofte sociale manipulationsteknikker til at narre folk til at afsløre fortrolige oplysninger.

Forståelse af disse teknikker er afgørende for at undervise i, hvordan man genkender og undgår dem.

Eksempler på social manipulation:

- En medarbejder deler loginoplysninger over telefonen med en person, der hævder at være fra IT-support.
- En medarbejder klikker på et link i en e-mail, der er tilsyneladende fra en ledelsesmedarbejder, hvilket fører til phishing-angreb.



Refleksion: Find et eksempel på hvor I har været udsat for social manipulation?




Vaner og bekvemmelighed

Mennesker har en tendens til at vælge den nemmeste vej, selvom det kan være usikkert. Identificerings- og adgangspåbeholdninger bør derfor designes med fokus på brugervenlighed for at minimere modstand mod implementeringen.

Eksempler på vaner og bekvemmelighed

- En medarbejder vælger at bruge en simpel adgangskode som "123456" eller "password" for at undgå besværet ved at huske en kompleks kode
- En medarbejder anvender den samme adgangskode på tværs af flere tjenester for at undgå besværet ved at huske forskellige koder. Det udgør en trussel, da kompromittering af én konto kan føre til adgang til andre konti.



Refleksion: Find et eksempel på hvor vaner og bekvemmelighed er en hindring for jeres sikre digitale adfærd?




Overbelastning af information

Når medarbejdere konstant bombarderes med information om sikkerhed, kan de blive overvældede, hvilket kan føre til passivitet eller ignorering af vigtige sikkerhedsprotokoller. Struktureret, relevant og letforståelig information er nøglen.

Eksempler på overbelastning af information

- Medarbejdere modtager daglige sikkerhedsadvarsler via e-mails eller pop-ups, men ignorerer dem på grund af overbelastning af information.
- På grund af informationsoverbelastning overser medarbejdere gentagne opfordringer til at opdatere software, hvilket resulterer i sårbare systemer, der ikke er beskyttet mod de seneste trusler.



Refleksion: Find et eksempel på hvor I mener I har været udsat for overbelastning af information?




“Det sker ikke for mig” syndrom

Mennesker har en tendens til at tro, at de ikke er mål for cyberangreb. Dette kan føre til forsømmelse af sikkerhedsforanstaltninger. Uddannelse bør adressere denne opfattelse og vise, at alle er potentielle mål.

Eksempler på “Det sker ikke for mig”:

- En leder ignorerer gentagne opdateringer til sikkerhedsprocedurer og -software, idet vedkommende tror, at virksomheden ikke er et mål for cyberangreb.
- En medarbejder undlader at lave regelmæssige sikkerhedskopier, da vedkommende tror, at data ikke vil blive kompromitteret. Dette kan føre til betydeligt datatab ved et angreb.




Refleksion: Find et eksempel på hvor
"det sker ikke for mig" har gjort sig
gældende hos jer..



Ingen konsekvenser ved overtrædelse

Hvis der ikke er klare konsekvenser for usikker adfærd, kan medarbejdere være tilbøjelige til at ignorere sikkerhedsprocedurer. Implementering af konsekvenser som en del af træningsprogrammet kan motivere til overholdelse.

- **Eksempler på ingen konsekvenser ved overtrædelse:**
- Medarbejdere, der gentagne gange bryder sikkerhedsprotokoller, oplever ingen konsekvenser. Dette reducerer motivationen for at overholde sikkerhedsreglerne.
- Medarbejder tager IKKE phishing-simulationer alvorligt, da der ikke er reelle konsekvenser ved at klikke på ondsindede links.




Refleksion: Find et eksempel på hvor
"ingen konsekvenser" har påvirket
jeres adfærd...



Tillid til teknologien

Mennesker stoler ofte for meget på teknologi og antager, at systemer altid vil beskytte dem. Det er vigtigt at understrege, at teknologiske løsninger ikke er fejlfri, og individuel opmærksomhed er afgørende.

- **Eksempler på tillid til teknologien:**
- En medarbejder gemmer følsomme dokumenter i en delt mappe under antagelsen om, at systemets indbyggede sikkerhedsforanstaltninger er tilstrækkelige til at beskytte dataene.
- En medarbejder tror, at systemet automatisk opdaterer og ignorerer manuelle sikkerhedsopdateringer.



Refleksion: Find eksempler på hvor
"tillid til teknologi" har betydning for
jeres digitale adfærd

Trusselsbillede / Risikoanalyse

		Konsekvenser				
		1 Ubetydelige	2 Mindre	3 Alvorlige	4 Meget alvorlige	5 Katastrofale
Sandsynlighed	5 Ofte	5	10	15	20	25
	4 Sandsynlig	4	8	12	16	20
	3 Sjælden	3	6	9	12	15
	2 Usandsynlig	2	4	6	8	10
	1 Meget usandsynlig	1	2	3	4	5

Mål for tiltag





SMART-Mål

Hvorfor det er vigtigt: Mål fastlægger retningen og formålet med cyber awareness-programmet. At have klart definerede mål hjælper med at fokusere indsatsen og evaluerer senere succes. Målene bør være konkrete, målbare, opnåelige, relevante og tidsbegrænsede (SMART).

S - Specific

M - Measuarable

A -Achievable

R - Relevant

T - Timed

Start med at identificere specifikke mål for programmet. Dette kan omfatte at definere ønsket adfærdsændring, måle effektiviteten af træningsmaterialer eller reducere specifikke risici. Gør målene konkrete og brug dem som retningslinjer for programmet.

For eksempel kan et mål være at reducere antallet af rapporterede phishing-klik med 30% inden for det næste år i medarbejdergruppe X.

Målgrupper





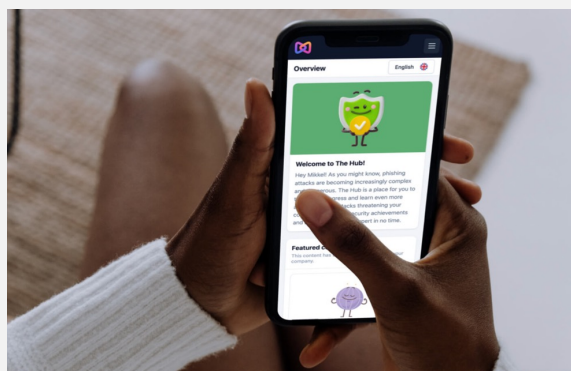
Målgrupper

- Målgrupper definerer, hvem programmet er rettet mod. Forskellige medarbejdergrupper kan have forskellige sikkerhedsbehov og risici.
- En målrettet tilgang hjælper med at skræddersy træningsmaterialer og strategier, hvilket øger effektiviteten af programmet.
- Tilpas træningen og kommunikationen til hver målgruppes specifikke behov. En bred tilgang tager hensyn til variationerne i medarbejdernes roller og ansvar.

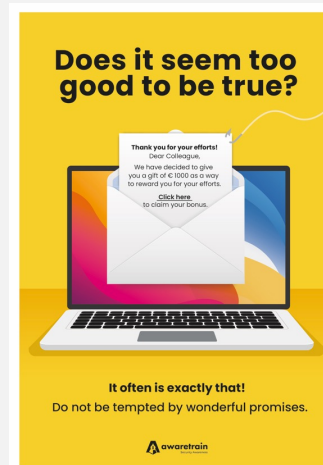
Valg af aktiviteter / kanaler



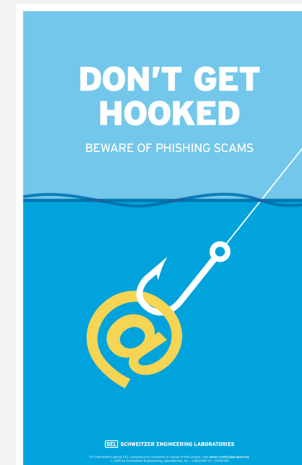
Fysiske kortspil



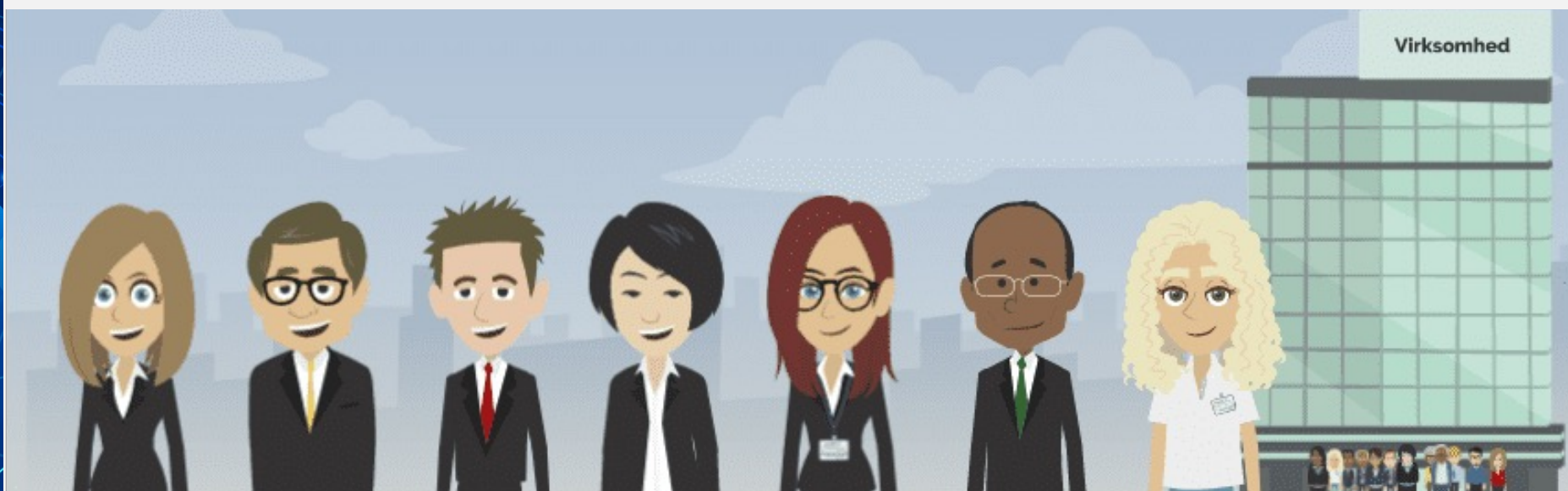
Interaktiv læring



Plakater



Roller og ansvar



Effektkæde

Aktivitet

Output

Resultater



Afrapportering





Afrapportering

- Afrapportering omfatter indsamling og analyse af data for at evaluere programmets effektivitet.
- Det er afgørende for at måle fremskridt, identificere områder til forbedring og demonstrere værdien af investeringen.
- Ved at definere klare nøgletal og rapporteringsmetoder på forhånd kan man kvantificere programmets indvirkning.
- For eksempel kan det inkludere regelmæssig rapportering af antallet af gennemførte træninger, resultater fra phishing-simulationer og feedback fra medarbejderne.



Afrapportering (eksempler=

1. Forbedring af phishing-awareness

Reducere antallet af klik på phishing-links i simulerede angreb med **30% inden for 6 måneder** i afdeling XYZ

Sikre, at mindst **90% af medarbejderne** genkender og rapporterer phishing-mails korrekt efter en awareness-kampagne på 3 måneder.

2. Deltagelse i træning

Sikre, at mindst **95% af medarbejderne** gennemfører XX awareness-træning inden for de næste **12 måneder**.

Øge deltagelsen i XX hands-on workshops fra **60% til 80%** inden for **9 måneder**.

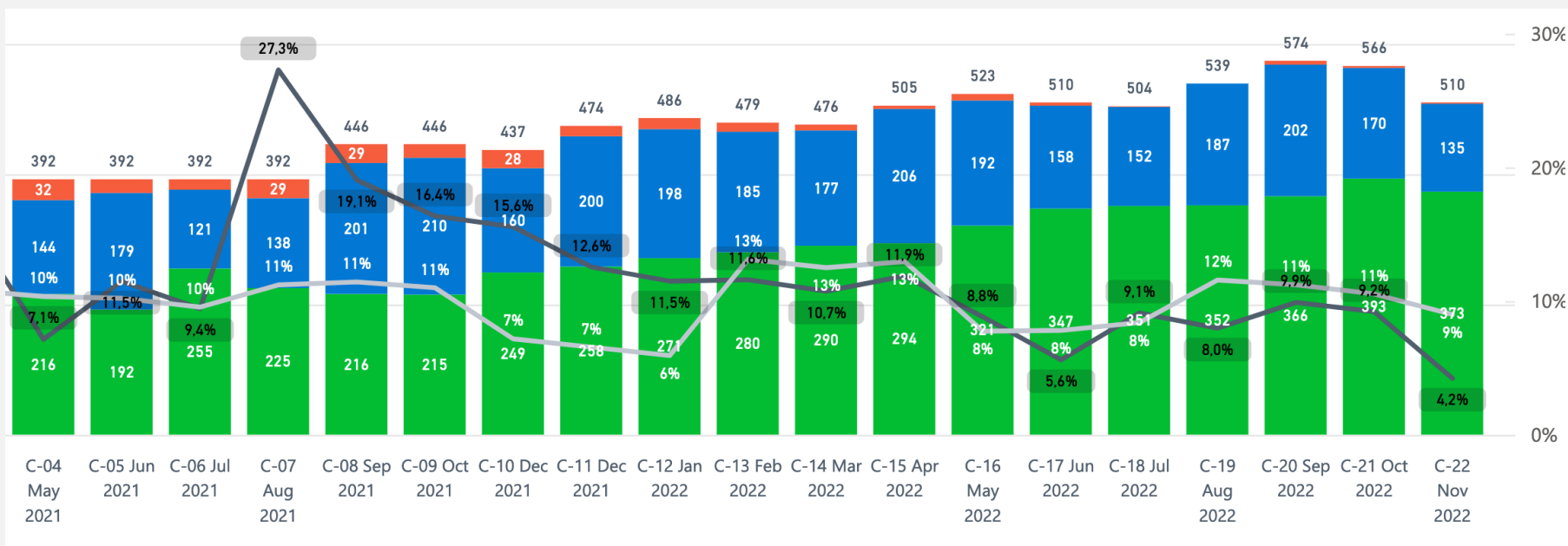
3. Rapportering af hændelser

Øge antallet af sikkerhedshændelser, der rapporteres til it-afdelingen, med **40% inden for 6 måneder**, som et resultat af øget træning i hændeshåndtering.

Reducere tiden fra identifikation til rapportering af en sikkerhedshændelse til gennemsnitligt **1 time inden for 6 måneder**.

Afrapportering (eksempel på phishing tool)

● Low Risk ● Medium Risk ● High Risk — Click rate — Click rate benchmarks



Datapunkter der kan måles på

Maturity Level	Description	Program Indicators	People Indicators	Time to Achieve	Metrics	Steps to Next Level
STAGE 1 No Security Awareness Program	Program does not exist. Employees have no idea that they are a target, that their actions have a direct impact on the security of the organization, do not know or understand organization policies, and easily fall victim to attacks. VALUE: None. Your organization is at high risk of failing to meet any compliance requirements and highly vulnerable to human-driven incidents.	<ul style="list-style-type: none">• There is no security awareness program.• Leadership does not discuss or care about security awareness.	<ul style="list-style-type: none">• Employees never discuss security or exhibit secure behaviors.	N/A	None	<ul style="list-style-type: none">• Identify the regulations or standards that you must adhere to.• Identify security awareness requirements for those standards.• Identify someone to roll out the required security awareness training.• Develop or purchase training that meets those requirements.• Deploy security awareness training.• Track and document who completes the training.
STAGE 2 Compliance Focused	Program is designed primarily to meet specific compliance or audit requirements. Training is limited to annual or ad hoc basis. Employees are unsure of organizational policies and/or their role in protecting their organization's information assets. VALUE: Your security awareness program meets the legal requirements your organization is required to adhere to. However your organization is not effectively managing its human risk.	<ul style="list-style-type: none">• Program is led by someone who is only dedicated part-time to the security awareness efforts.• Security awareness reports to CISO, compliance, audit, legal or human resources.• There is no strategic plan, training topics are ad hoc and deployed at random times.• Program has limited leadership support. Leadership's goal is to maintain compliance at minimum costs.• Security awareness is only considered during audits.• There is little coordination or partnership with other departments, such as communications and human resources.• Leadership perceives security as purely a technical issue.• Training is primarily once a year, often mandatory.• There is little to no communication to the workforce about security beyond the annual training.	<ul style="list-style-type: none">• People have a "let's get this over with" attitude.• People perceive security as something that the IT or security team takes care of—it's not their problem.• People feel security is something they have to do.• People have a negative perception of the security team, which is perceived as arrogant, too technical or perhaps even blockers.• People perceive security policies as confusing, difficult and as a blocker to their daily work responsibilities.• People often ignore policies and use their own solutions to get work done.	It depends on the standards, regulations or legal requirements you are attempting to adhere to. However, the overall effort is usually minimal, requiring nothing more than annual training.	<ul style="list-style-type: none">• Number/percentage of people that have completed training• Number/percentage of people that have signed Acceptable-Use Policy• Number of on-site training sessions in one year• Number/frequency of awareness materials distributed (newsletters, posters, etc.)	<ul style="list-style-type: none">• Identify and gain support of key leaders and stakeholders• Create Project Charter, identifying things such as scope, leadership, goals, objectives, assumptions, and constraints for the awareness program.• Identify who will be responsible for the awareness program. To ensure greatest success, that person should be dedicated full-time, have strong people skills, and report to and be part of the security team.• Identify the top human risks you will need to manage. Coordinate with Incident Response team, Security Operations Center, and/or Cyber Threat Intelligence team to assist with this. This may also require some type of human risk assessment.• Create an Advisory Board with members from key departments.• Identify the key behaviors that will mitigate and manage the top human risks.• Plan how you will communicate to, engage, and train your workforce on these key behaviors.• Develop and/or purchase your training materials.• Create execution plan with milestones to include metrics.• Have senior leadership announce program, then launch.
STAGE 3 Promoting Awareness and Behavior Change	Program identifies the top human risks to the organization and the behaviors that manage those risks. Program goes beyond just annual training and includes critical reinforcement throughout the year. More mature programs in this stage identify additional roles, departments or regions that represent unique risks that require additional or specialized role-based training. Content is communicated in an engaging and positive manner that encourages behavior change. As a result, people understand their role in cybersecurity, follow organizational policies and exhibit key behaviors to secure the organization. VALUE: Your organization is not only meeting its compliance requirements but is able to effectively identify, manage and measure its human risk.	<ul style="list-style-type: none">• The program is led by someone dedicated full-time to managing the security awareness program. In addition, this individual often has strong communication/people skills.• Security awareness reports to and is an integrated part of the security team.• Leadership understands and commits to the need for managing human risk.• There is a strategic plan that has identified the scope, goals, objectives, and justification for the program.• Through a risk assessment, and in partnership with different security team members (DFIR, SOC, CFI), the security team has identified and can explain the organization's top human risks and the behaviors that most effectively manage those risks.• Program has sufficient leadership support to provide resources necessary and has an executive champion.• Security awareness team actively partners and collaborates with various departments within organization, including communications, human resources, and help desk. Often this coordination is done through an advisory board.• Program goes beyond just annual training and includes continuous reinforcement throughout the year. It also usually includes a phishing simulation program.• More mature programs have identified different departments, roles or regions that represent increased or unique risks to the organization and require specialized or additional training (role-based training).• Program works to positively engage the workforce. Engagement is not based on mandatory training but creating training that people want to consume.	<ul style="list-style-type: none">• Employees understand that technology alone cannot protect them and that they have a responsibility to protect themselves and the organization.• People are reporting incidents or suspected attacks.• When security team pushes out information, people are asking them questions.• Employees are exhibiting the behaviors they are being trained on.• Employees begin to exhibit the same strong security behaviors at home and in their personal lives.• Employees are asking how their family can take the training.	Depending on the behaviors you are attempting to change, the longer it is to impact behaviors organization-wide within 3-6 months. For example, you can begin to see a dramatic drop in phishing click rates organization-wide if you do extensive phishing training and simulations. However, the more behaviors you are attempting to change, the longer it can take to change those behaviors organization-wide. This is one of the reasons it is so important to prioritize your top human risks, and the behaviors that manage those risks. The fewer behaviors you focus on, the more likely you can change those behaviors.	This stage is all about measuring the behaviors you care about and which behaviors are the most important to managing your risk. Some examples include: <ul style="list-style-type: none">• Phishing simulation click rates, number of repeat clickers and report rates• Number of lost or stolen laptops or mobile devices• Adoption rate of Password Managers or MFA• Percentage of employee passwords that could be cracked• Percentage of workstations that are securely locked down at night• Percentage of mobile devices that are current and/or screenlocks enabled• Number of accidental data loss events, such as data loss due to auto-complete in email or insecure Cloud accounts. NOTE: See the interactive metrics matrix for more examples. These metrics are ultimately driven by what behaviors are the most important to managing your human risk.	<ul style="list-style-type: none">• Establish a process to give leadership regular updates on the awareness program.• Identify a specific date when the security awareness program is reviewed and updated every year to include feedback by the Advisory Board.• During annual review and update, identify any new risks or behaviors required to manage human risk and new ways to communicate to, engage and train your workforce.• Security awareness team should be actively assisting with policy development to help ensure they are as simple as possible for the workforce.• Security awareness team should be actively assisting the security team in any outreach, communication and engagement efforts to include any new tool rollouts.• Some type of formal incentive program to recognize individuals, groups or departments excelling in cybersecurity and/or exhibiting key behaviors.
STAGE 4 Long-Term Sustainment and Culture Change	Program has the processes, resources, and leadership support in place for a long-term sustainment, including (at a minimum) an annual review and an update of the program. As a result, the program is an established part of the organization's culture and is current and engaging. Program has gone beyond changing behavior and is changing the workforce's shared attitudes, perceptions and beliefs about cybersecurity. A strong security culture not only creates an environment where people are far more likely to exhibit secure behaviors, but promotes and helps ensure security is built into almost all operational aspects of the organization, exponentially increasing the overall security of the organization.	<ul style="list-style-type: none">• Program is led by someone dedicated full-time to managing the security awareness program and has a team of multiple full-time employees focusing on managing human risk.• Security awareness reports directly to the Chief Information Security Officer (CISO).• Program is actively reviewed and updated on an annual basis.• Leadership believes in and has invested in long-term support of the program. Program lead is regularly updating leadership on a monthly or quarterly basis.• Security team believes in investing in human controls equally as much as technical controls. There is a strong partnership between the security awareness team and different elements of the security team (SOC, DFIR, CFI, etc.).• Security ambassador/champion program is run by a dedicated program manager.• Security awareness team is helping in the development of security policies, processes and procedures to ensure they are easier to understand and comply with.• Security awareness team is helping the security team with all organization-wide security communications or security tool roll-outs.	<ul style="list-style-type: none">• Good security practices are baked into who we are and what we do.• Employees educate others on good security behaviors.• Employees start providing ideas or suggestions on how to improve security in the organization.• Employees or departments actively reach out to and request assistance or briefings by the security team.• Department leads and teams request security reviews/audits.• The security team and their security efforts are perceived as approachable, collaborative and helpful by the workforce.	Impacting your organizational culture takes much longer than impacting behavior. Impacting culture can take 3-10 years depending on the size, complexity and age of your organization and its culture (John Kotter, Leading Change). For this stage, we recommend not focusing on changing your organization's culture, but embedding security into and aligning with your organization's existing culture.	<ul style="list-style-type: none">• Survey people's attitudes, perceptions, and beliefs towards information security (this can be broken down by what people think about your security policies, your security team and your security training).• Conduct focus groups or interviews for deep dives into people's attitudes, perceptions and beliefs• Number of people/departments are requesting security briefings or updates• Number of people are submitting ideas on how to improve security.	<ul style="list-style-type: none">• Create a metrics dashboard that combines all the information/measurements from the different maturity levels.• Identify and align with leadership's strategic priorities.• Identify and align with any key strategic security frameworks or models.
STAGE 5 Strategic Metrics Framework	Program has a robust metrics framework aligned with and supporting organization's mission and business goals. Program is no longer just measuring and reporting on changes in behavior and culture, but ultimately how these changes are reducing risk and enabling leadership to achieve their strategic priorities. As a result, the program is continuously improving and able to demonstrate return on investment. VALUE: Your program is aligned with and actively supporting your leadership's strategic priorities and your organization's business goals/mission.	<ul style="list-style-type: none">• Program is coordinating with leadership to understand and align with the strategic security frameworks and models they use.• Security awareness works with business leaders to identify and align with their strategic priorities.• Metrics are collected on a regular basis, often automated.• Metrics are provided to senior leadership demonstrating value at a business level and showing alignment with strategic business priorities.• Metrics are aligned with the security framework(s) that your leadership has committed to.	Leadership actively requests and uses security awareness metrics to measure their organizational progress and/or compare departments across the organization.	This is a long-term effort aligned with your overall program, as you are continually updating and improving your ability to collect useful metrics that you can both act on and provide to leadership.	<ul style="list-style-type: none">• A metrics dashboard that tracks the key metrics covered in the previous stages• How these changes are impacting and reducing overall risk to the organization, which can be measure in strategic metrics such as<ul style="list-style-type: none">• Overall number of security incidents• Average time to detect an incident (attacker dwell time)• Average time to recover from an incident• Number of policy, audit or compliance violations• In addition, show leadership how the awareness program is aligned with and enabling strategic goals in any strategic security frameworks, like the NIST CSF.	

Dagens opgave

I har indtil 12.15 (inklusive frokost) til at vælge én af de fem case-virksomheder og udvikle et bud på en **awareness-strategi**. Strategien skal som minimum indeholde følgende elementer.

1. Trusler/Risiko: Definer de trusler, og dermed risici, som virksomheder står overfor og skal håndtere
2. Målgruppe: Definer ud fra truslerne - hvem virksomheden skal fokusere på, ift prioriterede målgrupper
3. Aktiviteter: Beskriv de tiltag, I foreslår som skal øge bevidstheden omkring sikkerhed og ændre adfærd
4. Kanaler: Angiv, hvilke kommunikationskanaler der skal bruges, og hvorfor.
5. Ansvar og ejerskab: Hvem anbefaler I står for hvad
6. Begrundelse: Forklar, hvorfor netop denne tilgang vil være effektiv for virksomheden ift ønskede effekt/output
7. Evaluering: Forklar hvordan I har tænkt jer at måle på indsatserne og dermed også forbedre løbende

I har 10 minutter til at præsentere jeres løsning for virksomhedens ledelse. Målet med præsentationen er at overbevise ledelsen om at allokere ressourcer fra deres budget til at implementere jeres strategi, og være tydelig omkring den ønskede effekt I vil skabe.



TAK FOR I DAG!