Stairway to security heaven

Fem trin til risikobaseret informationssikkerhed og adfærd

Testphishing, stærkere adgangskoder og låst skærm er blandt klassikerne, når virksomheder ruller cybersikkerhed og awareness ud. Klassikerne bidrager uden tvivl til en højere indsigt og bevidsthed blandt medarbejderne på disse generelle emner. Om de adresserer de relevante risici og rent faktisk flytter adfærd er der delte meninger om. Et stigende antal virksomheder er begyndt at efterspørge risikobaserede og målbare indsatser for styrket awareness, adfærd og sikkerhedskultur. Det er lige præcis hvad fem-trins modellen til risikobaseret informationssikkerhed og adfærd giver dig. Med denne simple metode kan du udarbejde en plan for dit arbejde, der sikrer, at du sætter ind, hvor risikoen er højest ved, at du kommunikerer med de rigtige mennesker, ad de rigtige kanaler, om de rigtige emner. Metoden gør dig endda i stand til at følge fremdriften og argumentere for økonomien.

Informationsaktiver, trusselsscenarier, svagheder og tekniske løsninger

Ved du allerede, hvilke trusler, der er mest relevante i jeres virksomhed og har du styr på de tekniske og digitale løsninger, der imødekommer dem? Så er dette forarbejde ikke så nødvendigt.

Hvis du derimod har en blind vinkel i forhold til informationsaktiver, trusselscenarier og digitale sikkerhedsløsninger, så kan det være en ide at foretage et par indledende knæbøjninger inden du træder op på fem-trins modellens første step.

Nogle virksomheder får foretaget modenhedsvurderinger eller andre former for informationssikkerhedsanalyser.

Hvis det er tilfældet i din organisation, kan du med fordel få fat i rapporterne.

De kan give dig et indtryk af virksomhedens sikkerhedsniveau og hjælpe med at svare på spørgsmålene. Men fortvivl ikke, hvis det ikke er tilfældet. Måske kan du i stedet tale med kyndige medarbejdere, der har indblik i sikkerhedssituationen og få et godt overblik?

På baggrund af dine indledende knæbøjninger, er du klar til første step i fem-trins modellen.

Det, du skal afklare, er blandt andet:

- Hvad er virksomhedens kerneleverance og hvilke processer og IT-systemer er de allermest nødvendige for kerneleverancen?
- Hvilke trusler og risici ser I, som de allermest relevante at beskytte jer imod, for at kunne sikre kerneleverancen?
- Hvilke personalegrupper arbejder med de vigtigste processer og IT-systemer og hvordan kan trusselscenarier og risici påvirke dem – og omvendt?

TRIN 01

Kommunikation og forandring

I nogle virksomheder er alle samlet på én matrikel. I andre er medarbejderne spredt over flere kontinenter. I nogle virksomheder arbejder alle ved en computer på et hæve-/sænkebord. I andre er meget af personalet på farten og har udelukkende adgang til smartphones.

Kommunikationsmulighederne varierer fra virksomhed til virksomhed. Således varierer mulighederne for at gennemføre forandringskommunikation også.

Men hvorfor taler vi om forandringskommunikation? Det gør vi, fordi, en virksomheds håndtering af risici handler om adfærd blandt medarbejderne.

Risici opstår, fordi nogen gør noget, de ikke skulle have gjort eller ikke gør noget, de skulle have gjort. Derfor er adfærdsforandringer det, du skal arbejde med, når du vil nedbringe en risiko. Information alene ændrer ingenting.

For, at vi kan ændre adfærden, bliver vi nødt til at afdække, hvordan vi når ud til medarbejderne med information, kommunikation, dialog, nudges og hvad der ellers skal til for, at dårlige vaner bliver til gode vaner og risiciene mindskes.

Det er det, dette trin handler om. Du skal gennemføre en workshop med medarbejdere, der ved noget om organisationskommunikation og change management.

Det kan være kommunikationsmedarbejdere, HR-medarbejdere eller andre, der er vant til at benytte forskellige former for kommunikationskanaler.

Det gælder om at danne et overblik over de formelle såvel som de uformelle kommunikationskanaler i virksomheden. Alt fra intranetartikler, fællesmails, townhalls, afdelingsmøder, infoskærme, opslag ved kaffemaskinerne og 1 til 1 med chefen.

Formålet er at skabe overblik over dine muligheder for at nå ud til medarbejderne – og dermed muligheden for at skabe grundlag, for at ændre deres adfærd. Resultaterne af afdækningen af kommunikationsmulighederne kommer i spil i trin fem.

PORTFOLIO

A Nyhedsbrev
B Intranetartikel
C Live-events
D Afdelingsmøde

Eksempel på kanaler og nominatorer.

Saml workshopdeltagerne og bed dem om følgende:

- List de formelle kommunikationskanaler i virksomheden (fx intranet, nyhedsmails, afdelingsmøder, townhalls o. lign.)
- List de uformelle kommunikationskanaler (fx opslag ved kaffemaskinen, samtaler i kantinen o. lign)
- Kategoriser kanalerne i envejs og dialogkanaler
- Vurder kanalerne i forhold til deres effektivitet (fx lederens beskeder ved 1:1 ift. intranetartikler)
- Giv en særlig plads til eksempler på konkrete tiltag, der har været anvendt med succes i virksomheden
- Giv hver kanal en nominator. Det kan f.eks være A, B, C osv.
- Saml oplysningerne i et regneark.

“Hvis ikke du baserer din Security Awareness på de mest relevante risici i din organisation, hvorfor så gøre det?”

“Mennesker er ikke rationelle, kommunikation alene ændrer ingen adfærd”

TRIN 02

Målgruppe analyse

Hvem er tæt på virksomhedens vigtigste aktiver? Hvem arbejder med fortrolige økonomiske informationer? Hvem kommer aldrig i nærheden af kerneaktiver, computere eller fortrolige data? Hvem kunne være skyld i eller selv blive ramt hvis et risikoscenarie indtræder? I andet trin skal du danne dig et overblik over virksomhedens forskellige grupper. Alt afhængig af virksomhedstypen og jeres risikoscenarier, kan du opdele efter funktioner, fagligheder, eller noget helt tredje.

Formålet er at sikre, at du får et fyldestgørende overblik over alle, der kan være relevante for virksomhedens informationssikkerhed. Det er vigtigt at undgå tunnelsyn, så du ikke kun fokuserer på for eksempel topledelsen, finansafdelingen og personer med adgang til fortrolige data. Derfor gælder det om at opnå det brede perspektiv, så du ikke overser en væsentlig gruppe, som det kan vise sig at være afgørende for informationssikkerheden.

Her kan det være en fordel at skæve til jeres vigtigste risikoscenarier. Når I taler om dem, kan der dukke målgrupper op, som I ikke først havde tænkt på. Ligesom i første trin, skal du gennemføre en workshop, men denne gang kan det være nogle andre deltagere. Du skal bruge et bredt udsnit af indsigtsfulde repræsentanter fra forskellige dele af virksomheden, der har viden om målgrupper, adfærd og risikoscenarier.

Formålet med workshoppen er at danne dig et overblik over medarbejdergrupperne og beskrive de enkelte gruppers karakteristika. Det er grundlaget for at kunne vurdere gruppens relevans i et informationssikkerhedsperspektiv.

De forskellige karakteristika kan være:

- Om de arbejder med computere, tablets eller smartphones
- I hvilket omfang de har adgang til fortrolige oplysninger
- Om de har administratoradgang til særlige systemer
- Om de rejser meget og arbejder på farten osv.

MÅLGRUPPE	ÅRSAG
Servicedesk	Kontaktdata eksponeret udadtil. Har mulighvis priviligerede adgange, er kan gøre dem til targt for hackere.
Kundecenter	Kontaktdata eksponeret udadtil. Mulighed for utilfredse brugere.
Priviligerede brugere	Priviligerede adgange kan udgøre target for hackere. Høj konsekvens hvis deres adgange bliver misbrugt.

Eksempel på, hvordan resultatet af din workshop kan se ud.

Her er arbejdspunkterne for workshoppen:

- Bed deltagerne skrive alle de medarbejdergrupper, de kan komme i tanke om, ned på post-it lapper
- Hæng grupperne på en tavle og beskriv hvorfor de er interessante. Evt. med en reference til jeres risikoscenarier.
- Bed deltagerne skrive karakteristika til hver gruppe på post-it lapper. Servicedesk kan f.eks. være interessant, fordi de har mange adgange og en bred kontaktflade, og kundecentret er ofte eksponeret ud af organisationen.
- Hæng disse karakteristika op ud for hver gruppe, find overlap og find de mest rammende beskrivelser
- Saml alle oplysningerne i en ny fane af dit regneark

TRIN 03

Risikoanalyse og Risk Services

Nu har du dit overblik over samtlige medarbejdergrupper og deres karakteristika. Dermed er du klar til risikoanalysen og risk savviness.

Formål med trinnet:
Formålet med risikoanalysen er at prioritere og målrette din informationssikkerheds- og adfærdsindsats mod de grupper, hvis adfærd kan få de mest kritiske følger for virksomheden.

I dette trin tager vi udgangspunkt i en klassisk tilgang til risikovurderingen ved at kombinere sandsynlighed og konsekvens. Vi vurderer sandsynligheden for, at den enkelte gruppe ved en kombination af angreb og adfærdsfejl kan blive skyld i et nedbrud eller læk.

Det sammenholder vi med de konsekvenser det kan få, hvis det sker. Vi placerer de enkelte grupper i en klassisk risikomatrix, hvor grupperne i øverste højre hjørne er dem, hvor der både er høj sandsynlighed og høj konsekvens. Det er lige præcis de grupper, der bliver vores primære målgrupper.

Resultatet af den del af workshoppen kan se ud som dette skema, hvor vi tager udgangspunkt i en 6 trins risikomatrice.

Herefter er det tid til at vurdere vores primære målgruppers savviness. Vi bruger savviness-begrebet som betegnelse af gruppernes forståelse af egen risikoprofil og adfærd. Parametrene man kan bruge, er blandt andet gruppens IT-kyndighed, tilbøjelighed til at følge procedurer, lydhørhed overfor ledelsesudmeldinger, forandringsparathed og ansvarsfølelse.

Formål
Formålet med at vurdere gruppernes savviness er at skabe et værdifuldt videns grundlag om de enkelte grupper, som bliver afgørende i vores valg af metoder til at påvirke og ændre deres adfærd.

Når du skal vurderes målgruppernes risk savviness kan du tage udgangspunkt i parametrene nedenfor eller lave dine helt egne, der passer bedre til din organisation.

Vi giver de enkelte grupper en vurdering fra A til E, hvor A er høj savviness og E er lav savviness.

Til slut i workshoppen skal I vurdere, hvor på jeres matrix risikoaccept niveau skal ligge. Dvs. den streg, der skal trækkes og afgøre hvilke målgrupper, I skal arbejde med.

Trin tre løser du i endnu en workshop. Igen med indsigtsfulde medarbejdere i virksomheden. Denne gang kan det f.eks. være repræsentanter fra IT-sikkerhed, Servicedesk og lignende faggrupper.

DEFINITION	
A	God forståelse for egen risikoprofil. Tager ansvar for risici relateret til rolle og arbejder målrettet med at mindske dem gennem egen adfærd. Gode IT-kundskaber
B	Forstår egen rolle og ansvar. Har en grundlæggende forståelse for behovet for at arbejde IT sikkert. Kender til og følger adfærdskodeks. Gode IT-kundskaber.
C	Forstår egen rolle og til dels ansvar. Støtter op omkring IT sikkerhed, så længe det ikke tager for meget tid. Nogenlunde IT-kundskaber.
D	Ikke begreb om egen rolle. Ingen kendskab til risici relateret til egen adfærd. Synes IT sikkerhed er noget IT bør fikse. Ikke de store IT-kundskaber.

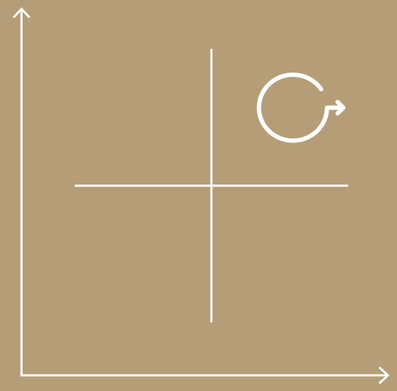
Eksempel på parametre til brug for risk savviness vurdering.

MÅLGRUPPE	KONSEKVENS	SANDSYNLIGHED
Servicedesk	5	3
Kundecenter	1	6
Priviligerede brugere	6	4

Eksempel på regneark efter trin 3.

MÅLGRUPPE	SAVVINESS
Servicedesk	B
Kundecenter	A
Priviligerede brugere	C

Vurderingen af målgruppernes saviness i en ny fane i jeres Excel-ark.



Her er arbejdspunkterne i workshoppen:

- Tegn en stor matrix på en tavle hvor du har ”konsekvens” ud af y-aksen og ”sandsynlighed” ud af x-aksen. Det er vigtigt, at du bruger de samme parametre, som I normalt bruger i jeres risikovurderinger.
- Tag grupperne en for en og diskutér med deltagerne, hvor den enkelte gruppe skal placeres i matrixen.
- Når alle grupper er placeret, skal I genbesøge grupperne for at vurdere de enkelte gruppers savviness.
- Når alle grupper er vurderet, laver i en streg i matrixen, der skal illustrere risikoaccepten. De målgrupper, der ligger over stregen er dem, I vil koncentrere jer om fremover.
- Noter resultater og observationer i endnu en fane i dit regneark

TRIN 04

Adfærdsanalyse

Efter tredje trin sidder du tilbage med et målrettet fokus på de grupper, som er vigtigst i et informationssikkerhedsperspektiv. Ved at ændre deres eventuelle dårlige sikkerhedsvaner til gode vaner, løfter du for alvor virksomhedens sikkerhedsniveau.

Formålet med dette fjerde trin er at identificere uhensigtsmæssigheder i de udvalgte medarbejdergruppers adfærd i forhold til jeres ønske om at arbejde informationssikkert.

I første omgang skal du have identificeret adfærdsmønstre, som skal styrkes eller ændres.

Kast et blik på beskrivelserne af målgrupperne i andet trin. Her har du måske noteret, at HR-medarbejderne ofte arbejder med personfølsomme oplysninger og derfor kan risikere at blive skyld i et databrud, hvis de ikke opbevarer og deler oplysningerne sikkert. Så kan det være relevant at fokusere på, om der er de rette procedurer for at gemme og dele filer, og om medarbejderne følger dem.

Hvis der er tale om en gruppe, der arbejder med fortrolige data og samtidig er meget på farten, kan du overveje: Hvordan arbejder de, når de rejser og når de er på fremmede destinationer? Er der handlinger, der kan ændres, så sikkerheden styrkes?

Der kan være flere metoder at benytte i fjerde trin, fx interview, fokusgrupper eller observationer af arbejdspraksis. Fælles for dem er, at det handler om at identificere uhensigtsmæssig konkret adfærd, der skal ændres til informations sikker adfærd.

Parallelt med analysearbejdet i 4. trin, kan du med fordel undersøge, om det er et problem, der skal løses kommunikativt eller om man kan løse det teknisk – derved kan man undgå den menneskelige faktor.

Måske er der planer om at indføre et system, der gør det umuligt at logge på som administrator direkte på en server eller en scanner, der alarmerer når persondata gemmes i uautoriserede systemer.

Undersøg, hvilke tekniske og digitale sikkerhedsforanstaltninger, der kan være under opsejling.

I dette trin skal du:

- Udarbejde en adfærdsanalyse
- Danne et overblik over andre sikkerhedsforanstaltninger, der er på vej, som kan mindske målgruppernes risikoprofil

Når du har identificeret eventuelle uhensigtsmæssige handlemønstre og kender den ønskede adfærd for hver af de prioriterede medarbejdergrupper, er det tid til femte trin.

TRIN 05

Strategi, plan og budget

I femte trin formulerer du mål, lægger strategi, beskriver en plan og lægger budget for indsatsen. Formålet er at få en konkret plan, der er til at eksekvere i praksis og som vil føre til konkrete adfærdsændringer og dermed mindske jeres risici. Ved at følge planen, vil du kunne dokumentere specifikke adfærdsændringer, som styrker sikkerhedsniveauet.

Først skal du sætte konkrete mål for de enkelte målgrupper:

- Hvilke ændrede adfærdsmønstre skal du kunne måle som resultat af indsatsen?
- Er der færre der klikker på links og flere der rapporterer mistænksomme e-mails?
- Er der færre observationer om mulige persondatabrud?
- Gemmes dokumenter korrekt og bliver de delt på sikker vis?
- Bliver alle computere låst, hver gang medarbejderne forlader deres pladser?

Dernæst skal du lægge strategien for, hvordan du opnår de konkrete mål. Her skal du bruge din liste af kommunikationskanalerne. Kombiner med målgruppernes karakteristika og deres savviness. Det giver dig et grundlag for at vurdere, hvordan du når ud til den enkelte målgruppe og en ide om hvad, der eventuelt vil virke for at få den pågældende gruppes opmærksomhed.

Organisationer og medarbejdergrupper er forskellige - og derfor er der ikke én måde at kommunikere med målgrupperne så de ændrer adfærd. Så nu er det op til dig at finde ud af, hvad der skal til for, at en given gruppe ændrer vaner og følger sikre processer.

MÅLGRUPPE	ÅRSAG	PORTFOLIO	KONSEKVENS	SANDSYNLIGHED
Servicedesk	Kontaktdata eksponeret udadtil. Har muligvis priviligerede adgange, der kan gøre dem til target for hackere	A+B	5	3
Kundecenter	Kontaktdata eksponeret udadtil. Mulighed for utilfredse brugere.	C	1	6
Priviligerede brugere	Priviligerede adgange kan udgøre target for hackere. Høj konsekvens hvis misbrugt.	B+C	6	4

Udfyld dit regneark med målgrupper, mål, indsats for at ændre adfærd og prisen på indsatsen.

Sæt indholdet i en tidsplan, saml budgettet og fordel ressourcer til at drive indsatsen.

Nu har du en direkte mapning imellem målgrupperne, den risiko, de udgør, samt den plan og det budget, der skal til for at flytte det i den rigtige retning.

Det betyder, at du også har et rigtigt godt udgangspunkt for at opnå ledelsesopbakning og en helt konkret plan, der kan føres ud i livet.

I dette trin skal du:

- Gøre dit regneark færdigt
- Sætte indholdet i en tidsplan
- Indsamle priser, estimere og udarbejde dit budget
- Lave en visuel præsentation med et overblik over hvad nedbringelse af den enkelte risikofyldte adfærd vil koste i timer og kr. og hvornår den bliver udført

Nu har du en konkret plan for hvordan du kan ændre og optimere IT-sikkerheden i din virksomhed.

Principper er afgørende for at din mission lykkes:

- Lederne skal gå forrest med det gode eksempel
- Medarbejderne skal vide, hvorfor indsatsen er vigtig
- De skal forstå, hvorfor tidligere adfærd udgør en sikkerhedsrisiko
- Det skal være umuligt, besværligt eller svært karriereskadende at fortsætte en uhensigtsmæssig adfærd
- Det skal være nemt at følge hensigtsmæssige procedurer
- Medarbejderne skal anerkendes for at ændre adfærd og roses for at bidrage til at beskytte virksomheden

Besøg sikkerhedogpopcorn.dk,
hvor vi popper ideer om informations-
sikkerhed.

Her nørder vi i security awareness,
kommunikation, adfærdsdesign og
informationssikkerhedskultur.

Om os

Fægter med kuglepenne mod cyberkriminelle

Philippe er alt andet end computerekspert. Faktisk er han i mange henseender inkompatibel med teknik og IT.

Til gengæld ved han noget om kommunikation, adfærd og dynamikker i store organisationer.

Han har beskæftiget sig med organisationskommunikation, forandringer og adfærd i snart 2 årtier – og de seneste fire år med informationssikkerhed som omdrejningspunkt.

Han har gennemført kommunikations- og adfærdsindsatser i blandt andet Ørsted, Novozymes og DSB.

Philippe er tilknyttet kommunikations- og adfærdsbureauet Operate A/S.

Ud over erfaringer fra styrelser, bureauer, uddannelsesinstitutioner og energisektoren, har Philippe en uddannelse i Statskundskab, en master i medier og kommunikation, uddannet projektleder og kurser i retorik.

Kun en hacker-tåbe frygter ikke en bibliotekar

Sarah er oprindelig uddannet bibliotekar. Og her vil enkelte måske tænke grå page, fodslæbende sko og en brun lun striksweater.

I Sarahs tilfælde er virkeligheden en anden.

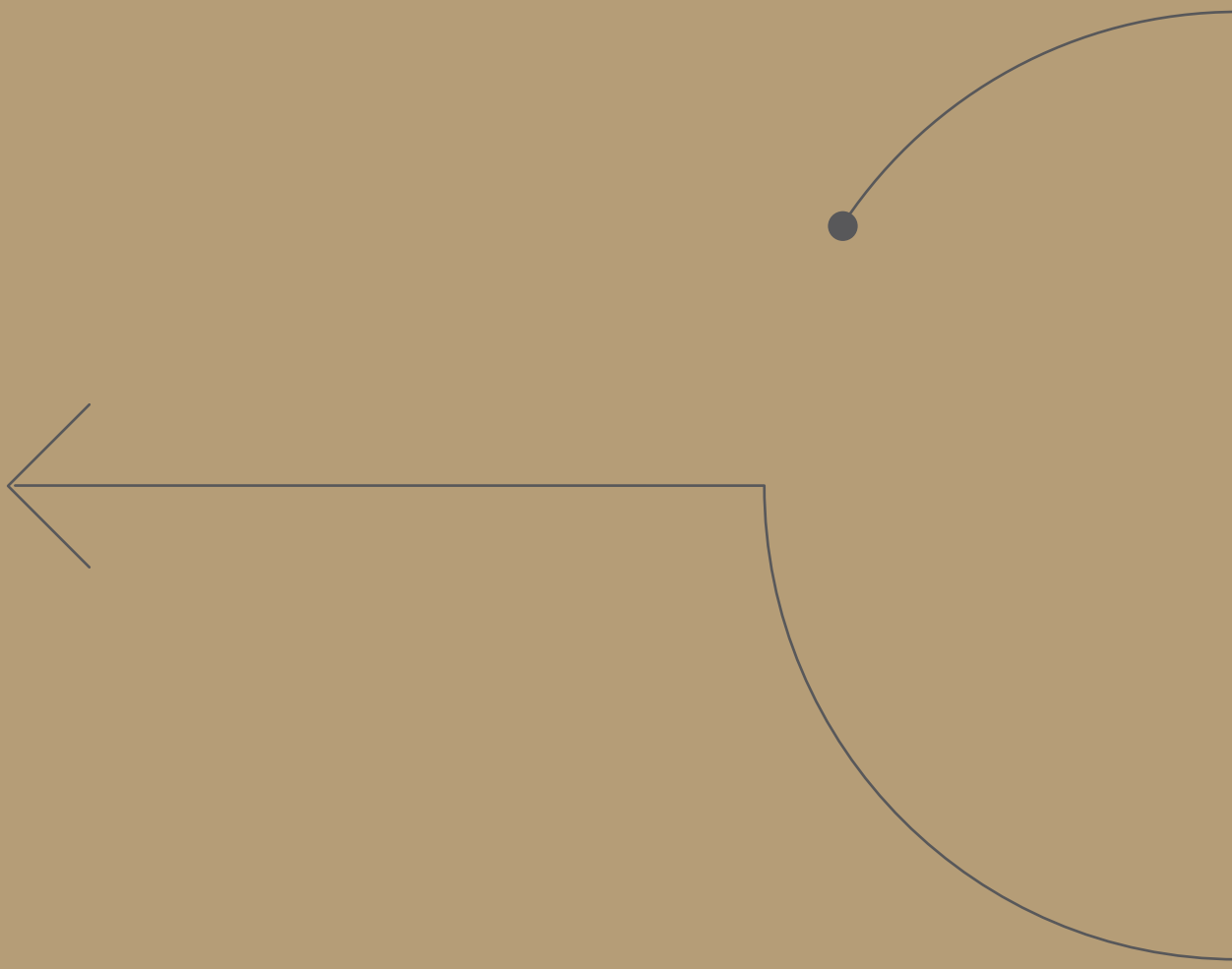
Sarah Aalborg er blandt landets fremmeste thought leaders, når det handler om informationssikkerhed, risikohåndtering og medarbejderadfærd.

Hun har arbejdet med sikkerhed i virksomheder som Oticon, Novozymes og DSB.

Sarah er en flittig anvendt speaker på it sikkerhedskonferencer og har blandt andet været keynote på digitaliseringsstyrelsens bootcamp og sluppet gennem nåleøjet som presenter på ISFs World congress.

Og det er om at spænde både hjelm og sikkerhedssele, når du møder Sarah … hun er en ustoppelig hvirvelvind af energi, ideer og løsninger.

Sarah har over 20 års erfaring i alle hjørner af IT og er uddannet både projekt og programleder. Dette er så toppet dette med en uddannelse som adfærdsdesigner, der giver en unik indgangsvinkel på IT sikkerhedsemnet



sikkerhedogpopcorn.dk