



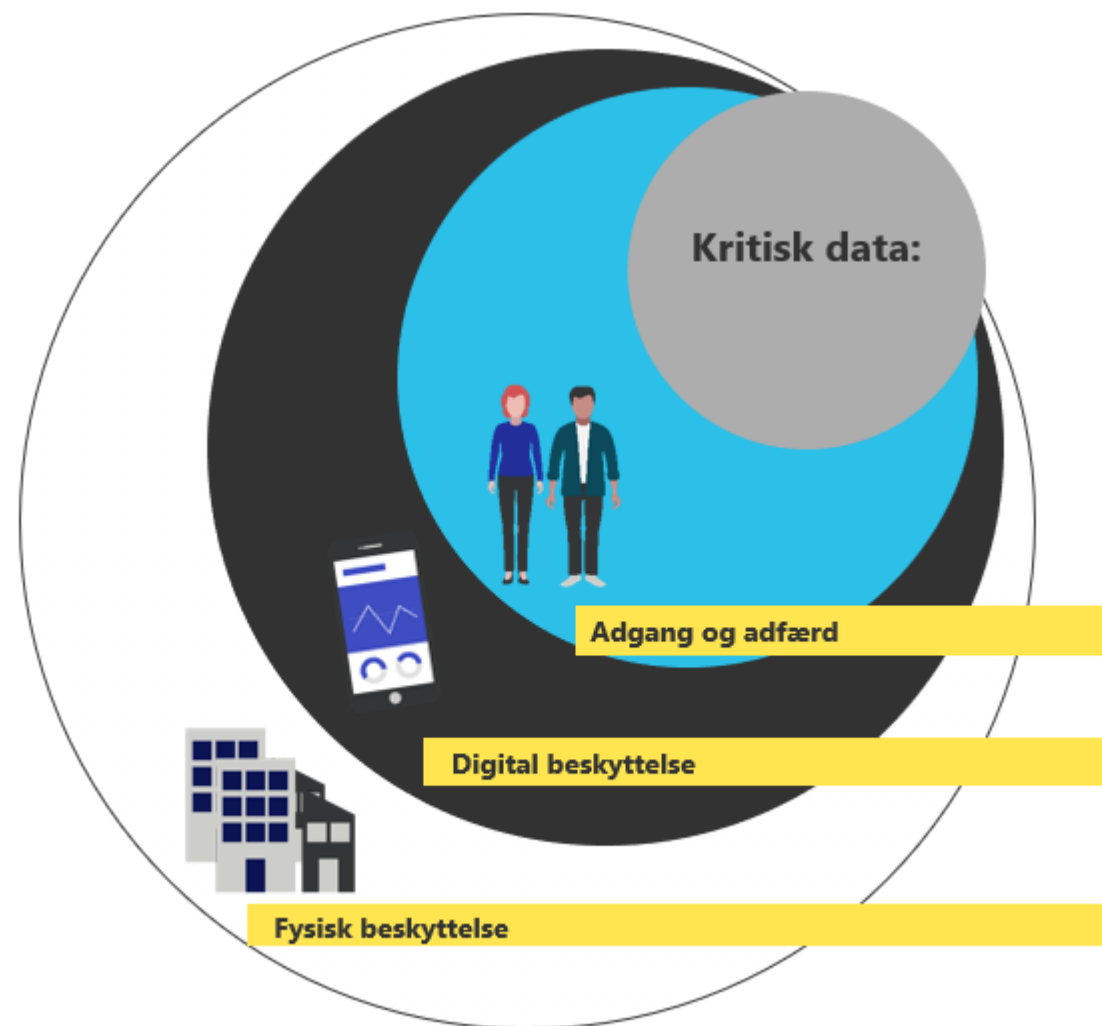
# Politikker og procedurer Beredskabsplaner Risikovurderinger Awareness

Carsten Jørgensen  
Department of Computer Science, DIKU  
September 19. 2025

UNIVERSITY OF COPENHAGEN



# IT sikkerhed er mange ting









# Fysisk sikkerhed – Drop Table



# Sikkerhedsledelse – eksempler på CISO opgaver

- Sikkerhedsstrategi
- Ledelsesrapportering
- Skrive og vedligeholde sikkerhedspolitikker
- Risikovurderinger og sikkerhedschecks
- Sikkerhedsvurderinger af nye løsninger
- Svare på spørgsmål om sikkerhed fra organisationen
- Koordinering af sikkerhedsaktiviteter
- Håndtering af intern og ekstern revision
- Awareness træning
- Holde øje med ændringer i risikobilledet
- ...

# Sikkerhed er mange ting – ISO 27001



## Sikkerhed

### **Organisatorisk**

Dokumentation, fx politikker, regler, processer, procedurer, vejledninger, logs, referater, rapporter, testresultater, målinger, evalueringer mv.

### **Adfærd**

Personale skal leve op til informationssikkerhedspolitik ved hjælp af vejledninger, uddannelse og awareness. Alle skal vide hvornår en hændelse skal rapporteres

### **Fysiske rammer**

De fysiske rammer skal beskyttes. De skal leve op til de krav, der sættes for at kunne beskytte systemer og information

### **Teknologisk sikring**

Består i styring af adgange, logning, back-up, kryptering osv, osv.



# **Sikkerhedsledelse: Lovgivning omkring sikkerhed**

# Sikkerhedsaktivitet på alle fronter

**GDPR**

**ENISA**

EU arbejder i en række arbejdsgrupper

Produkt certificeringer  
(RED, Maskindirektivet m.fl.)

**NIS2** – Når nedbrud og hændelser kan  
medføre "dramatiske konsekvenser"

**CER** – Critical Infrastructure Resilience

**ISO 27001**

NATO, internationalt

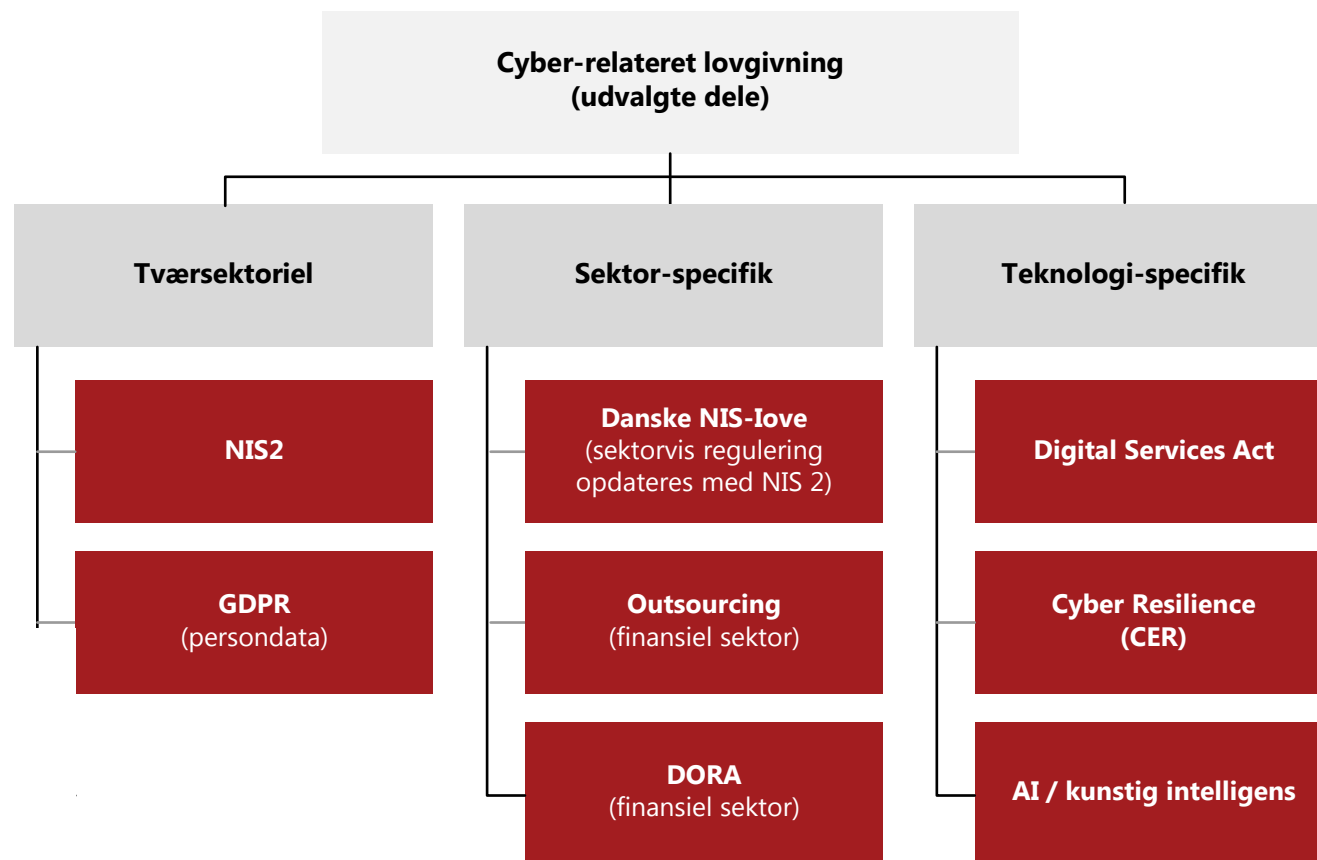
Ransomware og andre store  
sikkerhedshændelser til bestyrelserne





# Sikkerheds- lovgivning i EU

Direktivet er en del af et større reguleringsmæssigt kompleks på cyberområdet



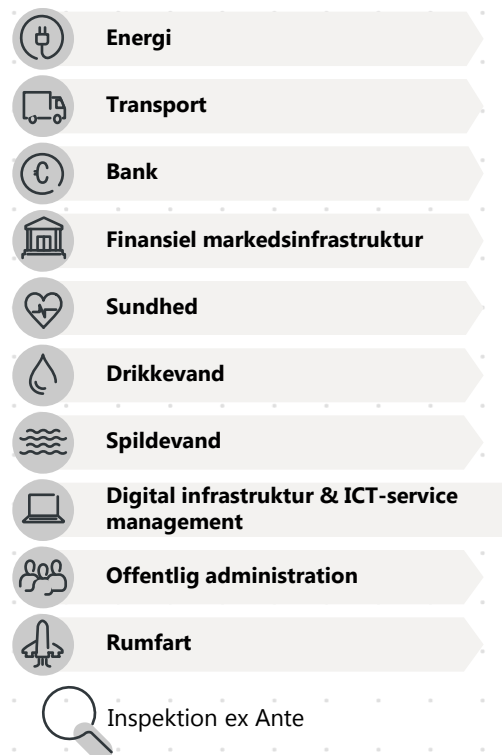
# Hvem bliver påvirket af NIS2?

NIS2 påvirker mere end **100.000 yderligere enheder**:

- Påvirker **medium** og **store virksomheder**; små virksomheder (<50 medarbejdere eller <€10m omsætning) bliver påvirkede, hvis de er af **afgørende betydning for samfundet**
- Klassificeret som **væsentlig** eller **vigtig** – bestemt af den sektor, hvor de opererer eller leverer tjenester
- Begge typer er omfattet af de samme krav for cybersikkerheds-risikostyring og rapportering; tilsyns- og sanktionsordningerne er forskellige



## Væsentlig



## Viktig



# Fem ting om NIS 2

- 1 Omfattende obligatoriske risikostyringsforanstaltninger – og et skift til en **risikobaseret tilgang**.
- 2 Første **rapportering** af hændelser skal ske inden for 24 timer, opfølgning inden for 72 timer og den endelige af rapportering skal falde inden for 1 måned.
- 3 Regelmæssig **uddannelse af ledelsen** i risikostyring af cybersikkerhed.
- 4 Den **øverste ledelse er ansvarlig** for overtrædelser. Myndighederne kan suspendere aktiviteter eller udøvelsen af deres rolle.
- 5 Bøder på op til **EUR 10 mio. eller 2%** af den samlede årlige omsætning på verdensplan.



# Indholdet i de 12 NIS2 krav uddybet

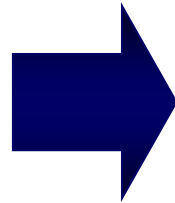
<b>1</b> Risikoanalyse og sikkerhedspolitikker for informationssystemer <ul style="list-style-type: none"> <li>Etablering og vedligehold af retningslinjer og politikker for efterlevelse NIS 2.</li> <li>Sikring af, at risikostyring er etableret, og at der på baggrund heraf træffes passende foranstaltninger for at styre risici.</li> <li>Sikring af, at ledelsen godkender foranstaltninger til styring af cybersikkerhedsrisici.</li> </ul>	<b>2</b> Håndtering af hændelser <ul style="list-style-type: none"> <li>Etablering og vedligehold af hændeshåndtering for alle systemer og netværk.</li> <li>Sikring af, at organisationen kan give tidlig varsel inden for 24 timer og hændelsesunderretning efter 72 timer.</li> <li>Monitorering af IT og OT skal forankres i og efterleve disse krav til hændeshåndtering.</li> </ul>	<b>3</b> Forretningskontinuitet, herunder backupstyring, it-katastrofeberedskab og krisestyring <ul style="list-style-type: none"> <li>Sikring af, at forretningskontinuitet (herunder krisestyring, katastrofegendannelse og krisestyring) er etableret og relevante mhp. at beskytte netværk og informationssystemer.</li> <li>Eftersyn af backupprocedurer og reetableringstest, samt etablering af rapportering for dette.</li> </ul>	<b>4</b> Sikkerhed i forsyningskæden, herunder direkte leverandører eller tjenesteudbydere <ul style="list-style-type: none"> <li>Etablering og eftersyn af, at sikkerhedskrav bliver systematisk inkluderet i leverandøraftaler.</li> <li>Verificering af, at leverandører lever op til definerede krav til sikkerhedsforanstaltninger, herunder under hensyntagen til specifikke sårbarheder og trusler.</li> </ul>
<b>5</b> Netværks- og systemsikkerhed ved erhvervelse, udvikling og vedligeholdelse <ul style="list-style-type: none"> <li>Etablering og eftersyn af effektiviteten af sikkerhedskrav ved erhvervelse, udvikling og vedligeholdelse af netværk og informationssystemer.</li> </ul>	<b>6</b> Sårbarhedshåndtering og offentliggørelse <ul style="list-style-type: none"> <li>Etablering og eftersyn af sikkerhedskrav og passende foranstaltninger for sårbarhedshåndtering af netværk og informationssystemer.</li> </ul>	<b>7</b> Politikker og procedurer til vurdering af effektiviteten af risikostyringsforanstaltninger <ul style="list-style-type: none"> <li>Etablering og eftersyn af, at der er passende politikker og procedurer til at vurdere effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici for netværk og informationssystemer.</li> <li>Herunder brugen af både tekniske, operationelle og organisatoriske foranstaltninger.</li> </ul>	<b>8</b> Grundlæggende computerhygiejnepraksis og cybersikkerhedstræning <ul style="list-style-type: none"> <li>Etablering og eftersyn af, at der er passende krav til computerhygiejnepraksisser og cybersikkerhedstræning mhp. at beskytte netværk og informationssystemer.</li> </ul>
<b>9</b> Politikker og procedurer for brug af kryptografi og kryptering <ul style="list-style-type: none"> <li>Etablering og eftersyn af, at der er passende politikker og procedurer for brug af kryptografi og kryptering mhp. at beskytte netværk og informationssystemer.</li> </ul>	<b>10</b> Personalesikkerhed, politikker for adgangskontrol og forvaltning af aktiver <ul style="list-style-type: none"> <li>Etablering og eftersyn af sikkerhedskrav og passende foranstaltninger for personalesikkerhed, adgangskontrolpolitikker og asset management mhp. at beskytte netværk og informationssystemer samt disses fysiske miljøer.</li> </ul>	<b>11</b> MFA eller kontinuerlig autentificeringsløsninger; sikret stemme-, video- og tekstkommunikation <ul style="list-style-type: none"> <li>Etablering og eftersyn af sikkerhedskrav og passende foranstaltninger for MFA eller kontinuerlig autentificeringsløsninger; sikret stemme-, video- og tekstkommunikation mhp. at beskytte netværk og informationssystemer.</li> </ul>	<b>12</b> Ledelsen skal følge regelmæssig færdigheds- og videnbaseret træning om cybersikkerhedsrisici <ul style="list-style-type: none"> <li>Sikring af, at ledelsen følger kurser for at opnå tilstrækkelige kundskaber for at identificere risici og vurdere metoderne til styring af cybersikkerhedsrisici og deres indvirkning.</li> <li>Sikring af, personale uddannes om cybertrusler, phishing og social engineering-teknikker mhp. at beskytte netværk og informationssystemer.</li> </ul>



# Sikkerhedsledelse

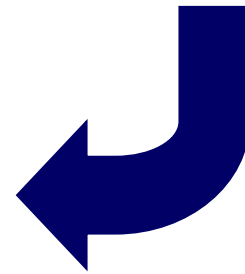
# Behovet for it-sikkerhed

**IT og cybersikkerhed -  
hvad er det  
rigtige niveau ??**



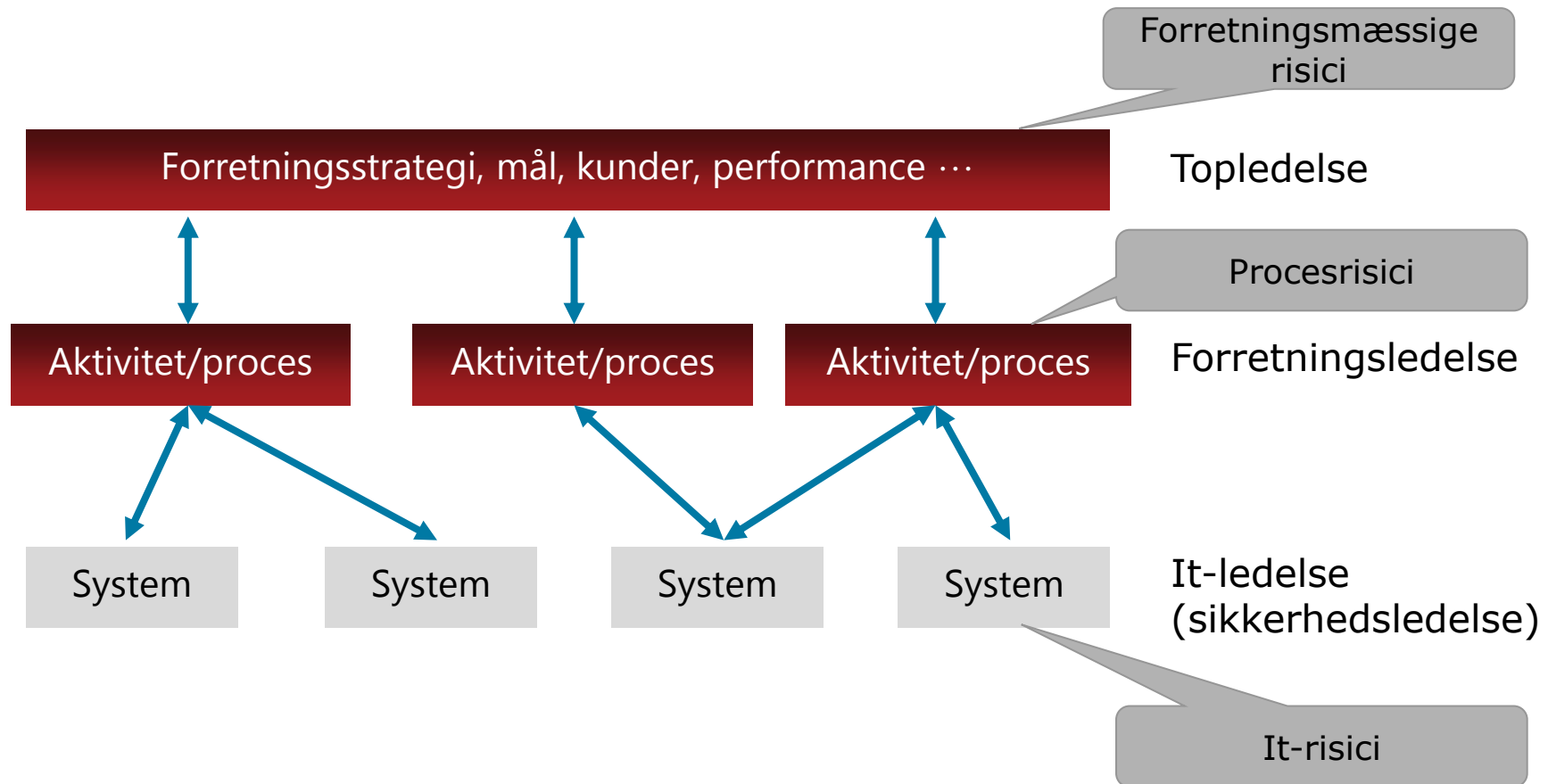
- Det kan være svært at afgøre, hvad det rette sikkerhedsniveau skal være.
- "Høj" sikkerhed er ikke altid nødvendigt
- "Lav" sikkerhed kan være katastrofalt !

**Det er  
forretningen og  
lovgivningen der  
stiller krav til  
sikkerhedsniveau**





# I forretningsmæssig kontekst





Politikker, procedurer, guidelines

# Sikkerhedspolitikker og procedurer

Må vi bruge ChatGPT på arbejdet?

Må Alice få admin-rettigheder til økonomisystemet?

Må jeg åbne port 81 fra Any til Any?

Må Bo rette direkte i databasen?

Må jeg sende dokumenterne i en mail til kunden?

Må udviklerne teste med produktionsdata?

Må jeg udlevere information over telefonen?

**Hvem tager beslutningen?**

**Hvad er beslutningen baseret på?**



# Sikkerhedsmål

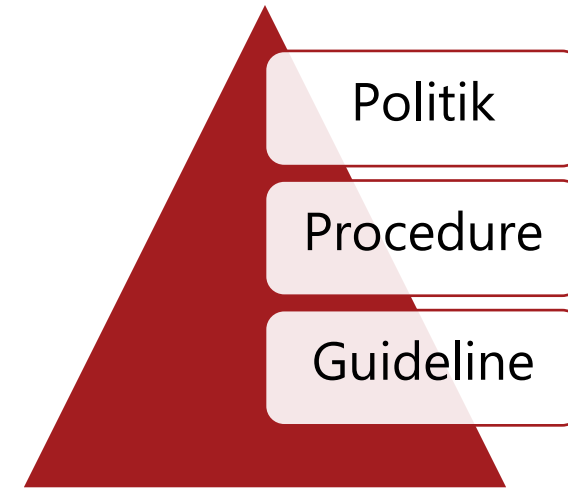
## **Sikkerhedspolitik :**

Definerer mål, det er strategien.  
Hvorfor, ikke hvordan.

## **Sikkerhedsguidelines:**

Detaljeret specifikation, definerer hvordan en sikkerhedspolitik skal implementeres i et specifikt produkt eller specifik situation.

Bruges som målepunkt for at vurderer om de udførende har gjort deres arbejde.



Note: Forskellige organisationer bruger forskellige termer, øverste niveau kan hedde f.eks. "Politik" eller "Strategi", men principper og hierarkiet er det samme

# Strategy - eksempel

## 1 Purpose

The Falck Group organization depends on IT systems to a great extent to achieve its daily operations and business goals.

This IT Security Strategy defines the directions for the IT Security Policies and Procedures necessary to maintain stable and trustworthy IT services to all business entities within the Falck Group.

The purpose of the IT Security Strategy is to:

- Ensure contractual obligations can be met, including ensuring that Falck Group can provide assistance in situations of emergency
- Minimize the risks of financial losses
- Maintain business system availability
- Ensure regulatory compliance
- Maintain customer and partner confidence
- Protect intellectual property and safeguard the Falck Group brand



# Sikkerhedspolitikker



## 8.9 Secure disposal or re-use of electronic equipment and other media

### Overwriting

Before equipment can be disposed or reused outside Falck Group all data must be securely overwritten using specialized software. Alternatively the storage media must be physically destroyed.

The standard “*delete*” and “*format*” functions do not remove data from electronic equipment. Therefore specialized disk or device “sanitation” software, such as the free DBAN software must be used to erase the data by completely overwriting the disk.



# Eksempler på dokumentation

Procedure for system dokumentation  
Procedure for Identifikation og Klassifikation af Informationsaktiver  
Procedure for Patch- Change- & Configuration Management  
Procedure for backup / sikkerhedskopiering  
Procedure for Informationsudveksling  
Procedure for fejlhåndtering & support  
Procedure for håndtering af følsomme oplysninger  
Procedure for data destruktion / data wipe  
Procedure for logning / kontrolspor  
Procedure for vedligehold og forbedringer  
Procedure for risiko og sårbarhedsanalyser  
Procedure for trussels vurderinger  
Procedure for Change Management / ændringsprojekter  
Procedure for funktionsadskillelse  
Procedure for Håndtering af eksterne Leverandører  
Procedure for Håndtering af eksterne samarbejdspartnere  
Procedure for Netværks- og system sikkerhed  
Procedure for Adgangs- og brugerstyring (IAM)  
Procedure for Sikkerhedshændelser / Incident Management  
Procedure for Fysisk sikkerhed  
Procedure for nød- og beredskabsplaner  
Procedure for Informations- og it-sikkerheds awareness / træning  
Procedure for databærende medier & mobilt udstyr  
Procedure for kryptering  
Procedure for beskyttelse mod vira, malware og ondsindet/uønsket programmel  
Procedure for brug af trådløse netværk  
Procedure for anskaffelse og udvikling samt vedligehold af it-systemer

...



# Formatet på dokumentationen er vigtig

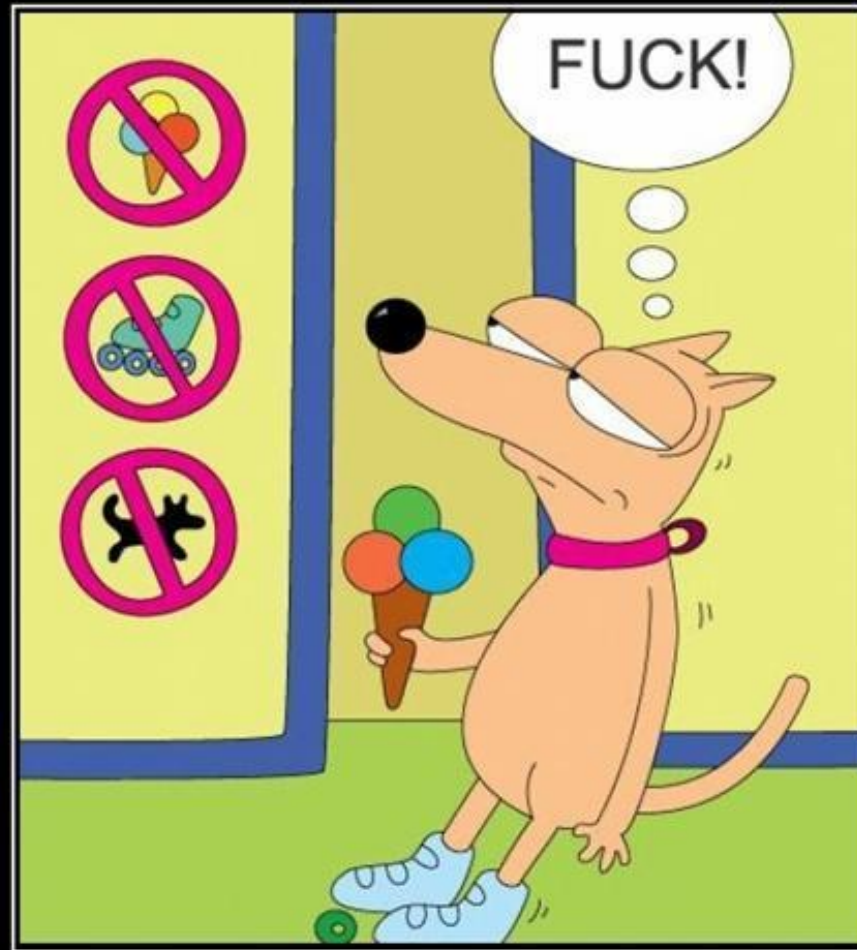




# **Beredskabsplaner**

## **Disaster recovery og Business continuity**

# Accidents happens



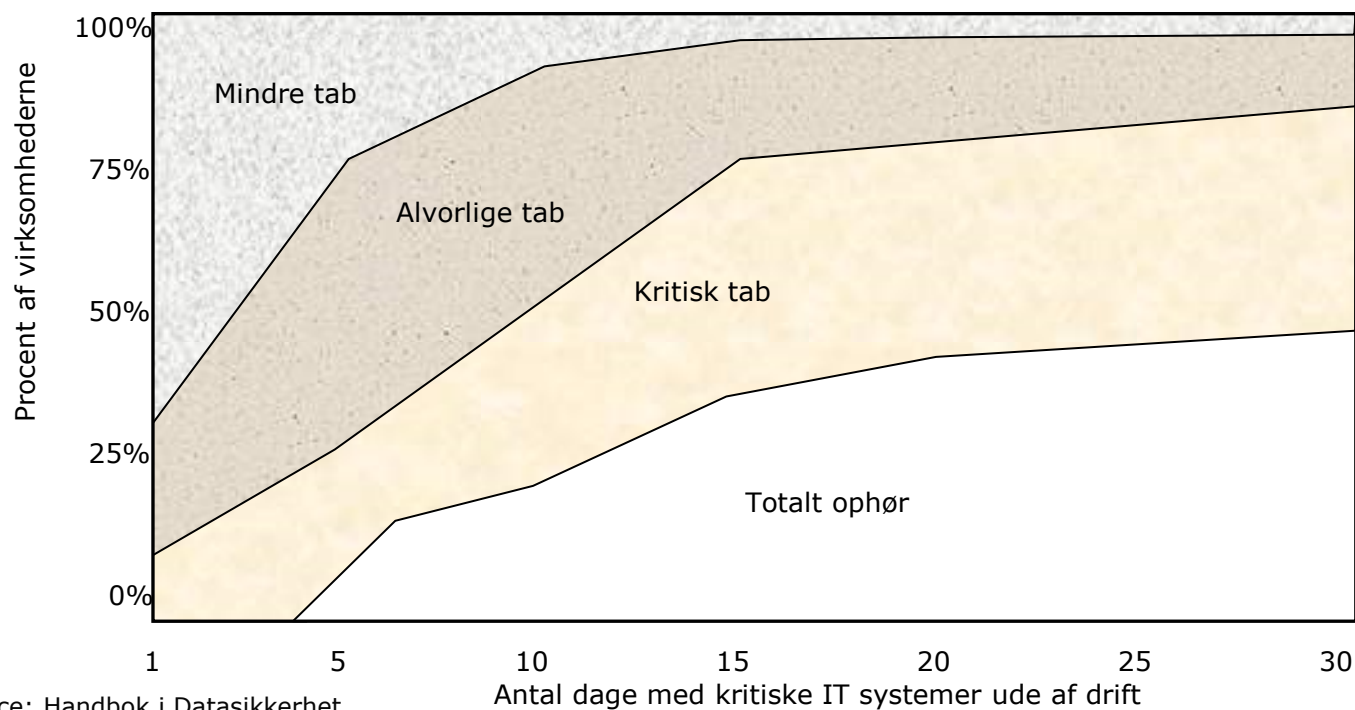
FUCK

Could you be any more unfortunate

# HVORFOR er beredskab vigtigt?

Nedbrud af IT-services vil have en stor betydning for mange virksomheders overlevelsessevne

Kan i nogen tilfælde true virksomhedens overlevelse



Source: Handbok i Datasikkerhet



SENESTE NYT **INDLAND** UDLAND PENGES POLITIK REGIONALT VEJRET

INDLAND

## AI data forsvundet i ransomware-angreb - Chili Klaus mistede sin hjemmeside

Dansk hostingudbyder er blevet ramt af et ransomwareangreb – kunder mistede data. Chili Klaus er en af dem.





# Brand i Apotekerforeningen



## It-chef efter brand i København: Godt vi fik remote backup

**En voldsom ildebrand i Apotekerforeningens bygning har raseret flere etager. Men udover nogle nedbrændte desktop-computere kan it-chefen tage situationen roligt på grund af fuld backup-løsning, fortæller han.**

AF [JESPER KILDEBOGAARD](#), TIRSDAG 04. MAJ 2010 KL. 13:16  
EMNER: [BACKUP](#) [DISASTER RECOVERY](#) [IT-DRIFT](#)

Ilden har ødelagt alt på de øverste etager i Dehns Palæ i København, hvor Dansk Apotekerforening holder til. Et potentielt mareridt for en it-ansvarlig, men ikke noget voldsomt problem for Niels Braae, Apotekerforeningens it-chef.

»Vi har fuld backup at det hele på en ekstern lokation, så vi mister ikke et eneste vigtigt bogstav. Og serverrummet står ikke i den del af bygningen, der brænder, så der er ikke noget centralt, der er ramt,« fortæller han via mobiltelefon tirsdag middag, mens brandvæsenet stadig kæmper for at få kontrol over ilden.



ISS-ansatte er ved at redde værdier ud af Dansk Apotekerforenings hovedkvarter i Dehns Palæ i Bredgade i København. (Foto: Kenneth Meyer)



# Når kunderne ikke kan betjenes som de plejer

- Hvor længe kan et helt eller delvis udfald af IT i forretningen accepteres?
- Hvordan og hvilke forretningsprocesser skal kunne afvikles ved en beredskabssituation?
- Er det overhovedet muligt at klare opgaverne uden IT?
- Hvor omfattende en situation skal beredskabet indrettes efter?
- Hvilke forebyggende foranstaltninger bør igangsættes for lettere at kunne håndtere en beredskabssituation?



# Case

# På forhånd

## Afbrydelser

Eskalering

Budgetter og regler for godkendelse

Information internt

Kontaktlister (internt og eksternt)

Pressekontakt

Adgang til dokumentation i krisesituation

Oversigt over hardware, incl telefoner

Procedurer for genetablering, incl. tidsestimater (TRP)

# Pause



**Words of Heart:** Dating app matching people through their passwords



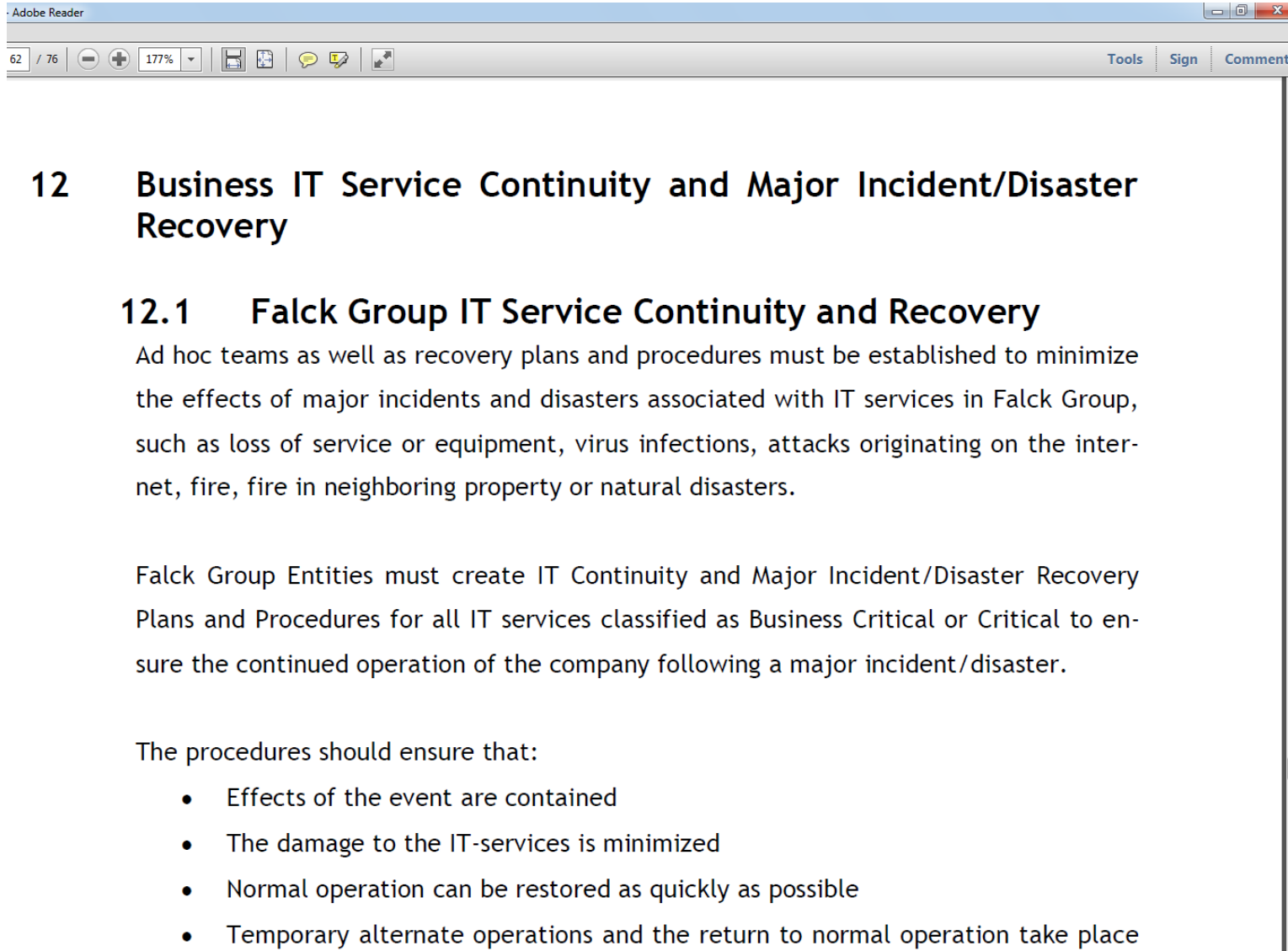
**FAIL**

## EVACUATION PLAN

Run and run  
as fast as you  
can



# Beredskab



Adobe Reader

62 / 76 177% Tools Sign Comment

12	<b>Business IT Service Continuity and Major Incident/Disaster Recovery</b>
12.1	<b>Falck Group IT Service Continuity and Recovery</b>
12.1.1	<b>Business IT Service Continuity and Recovery</b>
12.1.2	<b>Major Incident/Disaster Recovery</b>
12.1.3	<b>Business IT Service Continuity and Recovery</b>
12.1.4	<b>Major Incident/Disaster Recovery</b>
12.1.5	<b>Business IT Service Continuity and Recovery</b>
12.1.6	<b>Major Incident/Disaster Recovery</b>
12.1.7	<b>Business IT Service Continuity and Recovery</b>
12.1.8	<b>Major Incident/Disaster Recovery</b>
12.1.9	<b>Business IT Service Continuity and Recovery</b>
12.1.10	<b>Major Incident/Disaster Recovery</b>
12.1.11	<b>Business IT Service Continuity and Recovery</b>
12.1.12	<b>Major Incident/Disaster Recovery</b>
12.1.13	<b>Business IT Service Continuity and Recovery</b>
12.1.14	<b>Major Incident/Disaster Recovery</b>
12.1.15	<b>Business IT Service Continuity and Recovery</b>
12.1.16	<b>Major Incident/Disaster Recovery</b>
12.1.17	<b>Business IT Service Continuity and Recovery</b>
12.1.18	<b>Major Incident/Disaster Recovery</b>
12.1.19	<b>Business IT Service Continuity and Recovery</b>
12.1.20	<b>Major Incident/Disaster Recovery</b>
12.1.21	<b>Business IT Service Continuity and Recovery</b>
12.1.22	<b>Major Incident/Disaster Recovery</b>
12.1.23	<b>Business IT Service Continuity and Recovery</b>
12.1.24	<b>Major Incident/Disaster Recovery</b>
12.1.25	<b>Business IT Service Continuity and Recovery</b>
12.1.26	<b>Major Incident/Disaster Recovery</b>
12.1.27	<b>Business IT Service Continuity and Recovery</b>
12.1.28	<b>Major Incident/Disaster Recovery</b>
12.1.29	<b>Business IT Service Continuity and Recovery</b>
12.1.30	<b>Major Incident/Disaster Recovery</b>
12.1.31	<b>Business IT Service Continuity and Recovery</b>
12.1.32	<b>Major Incident/Disaster Recovery</b>
12.1.33	<b>Business IT Service Continuity and Recovery</b>
12.1.34	<b>Major Incident/Disaster Recovery</b>
12.1.35	<b>Business IT Service Continuity and Recovery</b>
12.1.36	<b>Major Incident/Disaster Recovery</b>
12.1.37	<b>Business IT Service Continuity and Recovery</b>
12.1.38	<b>Major Incident/Disaster Recovery</b>
12.1.39	<b>Business IT Service Continuity and Recovery</b>
12.1.40	<b>Major Incident/Disaster Recovery</b>
12.1.41	<b>Business IT Service Continuity and Recovery</b>
12.1.42	<b>Major Incident/Disaster Recovery</b>
12.1.43	<b>Business IT Service Continuity and Recovery</b>
12.1.44	<b>Major Incident/Disaster Recovery</b>
12.1.45	<b>Business IT Service Continuity and Recovery</b>
12.1.46	<b>Major Incident/Disaster Recovery</b>
12.1.47	<b>Business IT Service Continuity and Recovery</b>
12.1.48	<b>Major Incident/Disaster Recovery</b>
12.1.49	<b>Business IT Service Continuity and Recovery</b>
12.1.50	<b>Major Incident/Disaster Recovery</b>
12.1.51	<b>Business IT Service Continuity and Recovery</b>
12.1.52	<b>Major Incident/Disaster Recovery</b>
12.1.53	<b>Business IT Service Continuity and Recovery</b>
12.1.54	<b>Major Incident/Disaster Recovery</b>
12.1.55	<b>Business IT Service Continuity and Recovery</b>
12.1.56	<b>Major Incident/Disaster Recovery</b>
12.1.57	<b>Business IT Service Continuity and Recovery</b>
12.1.58	<b>Major Incident/Disaster Recovery</b>
12.1.59	<b>Business IT Service Continuity and Recovery</b>
12.1.60	<b>Major Incident/Disaster Recovery</b>
12.1.61	<b>Business IT Service Continuity and Recovery</b>
12.1.62	<b>Major Incident/Disaster Recovery</b>
12.1.63	<b>Business IT Service Continuity and Recovery</b>
12.1.64	<b>Major Incident/Disaster Recovery</b>
12.1.65	<b>Business IT Service Continuity and Recovery</b>
12.1.66	<b>Major Incident/Disaster Recovery</b>
12.1.67	<b>Business IT Service Continuity and Recovery</b>
12.1.68	<b>Major Incident/Disaster Recovery</b>
12.1.69	<b>Business IT Service Continuity and Recovery</b>
12.1.70	<b>Major Incident/Disaster Recovery</b>
12.1.71	<b>Business IT Service Continuity and Recovery</b>
12.1.72	<b>Major Incident/Disaster Recovery</b>
12.1.73	<b>Business IT Service Continuity and Recovery</b>
12.1.74	<b>Major Incident/Disaster Recovery</b>
12.1.75	<b>Business IT Service Continuity and Recovery</b>
12.1.76	<b>Major Incident/Disaster Recovery</b>
12.1.77	<b>Business IT Service Continuity and Recovery</b>
12.1.78	<b>Major Incident/Disaster Recovery</b>
12.1.79	<b>Business IT Service Continuity and Recovery</b>
12.1.80	<b>Major Incident/Disaster Recovery</b>
12.1.81	<b>Business IT Service Continuity and Recovery</b>
12.1.82	<b>Major Incident/Disaster Recovery</b>
12.1.83	<b>Business IT Service Continuity and Recovery</b>
12.1.84	<b>Major Incident/Disaster Recovery</b>
12.1.85	<b>Business IT Service Continuity and Recovery</b>
12.1.86	<b>Major Incident/Disaster Recovery</b>
12.1.87	<b>Business IT Service Continuity and Recovery</b>
12.1.88	<b>Major Incident/Disaster Recovery</b>
12.1.89	<b>Business IT Service Continuity and Recovery</b>
12.1.90	<b>Major Incident/Disaster Recovery</b>
12.1.91	<b>Business IT Service Continuity and Recovery</b>
12.1.92	<b>Major Incident/Disaster Recovery</b>
12.1.93	<b>Business IT Service Continuity and Recovery</b>
12.1.94	<b>Major Incident/Disaster Recovery</b>
12.1.95	<b>Business IT Service Continuity and Recovery</b>
12.1.96	<b>Major Incident/Disaster Recovery</b>
12.1.97	<b>Business IT Service Continuity and Recovery</b>
12.1.98	<b>Major Incident/Disaster Recovery</b>
12.1.99	<b>Business IT Service Continuity and Recovery</b>
12.1.100	<b>Major Incident/Disaster Recovery</b>

12 **Business IT Service Continuity and Major Incident/Disaster Recovery**

12.1 **Falck Group IT Service Continuity and Recovery**

Ad hoc teams as well as recovery plans and procedures must be established to minimize the effects of major incidents and disasters associated with IT services in Falck Group, such as loss of service or equipment, virus infections, attacks originating on the internet, fire, fire in neighboring property or natural disasters.

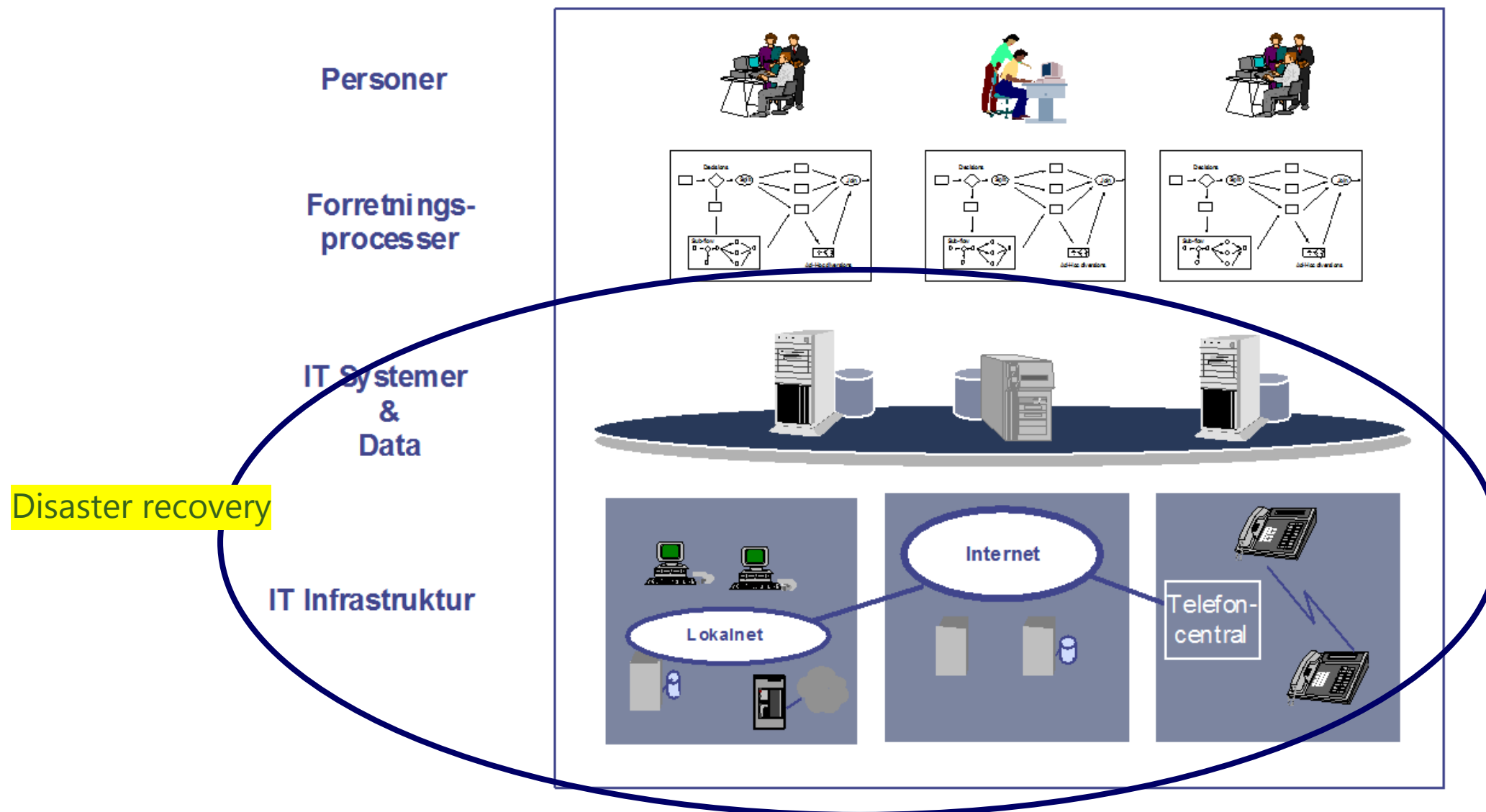
Falck Group Entities must create IT Continuity and Major Incident/Disaster Recovery Plans and Procedures for all IT services classified as Business Critical or Critical to ensure the continued operation of the company following a major incident/disaster.

The procedures should ensure that:

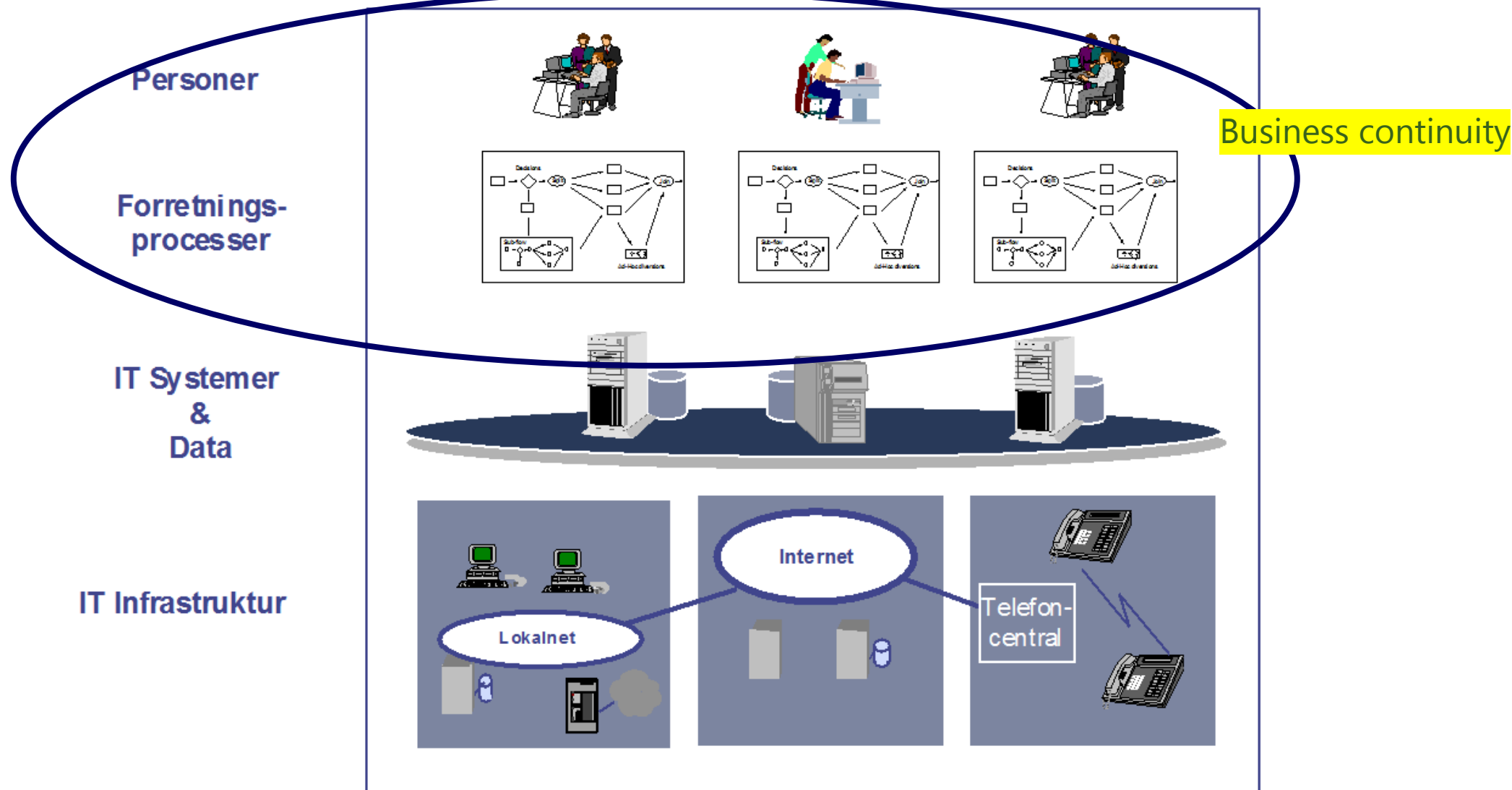
- Effects of the event are contained
- The damage to the IT-services is minimized
- Normal operation can be restored as quickly as possible
- Temporary alternate operations and the return to normal operation take place



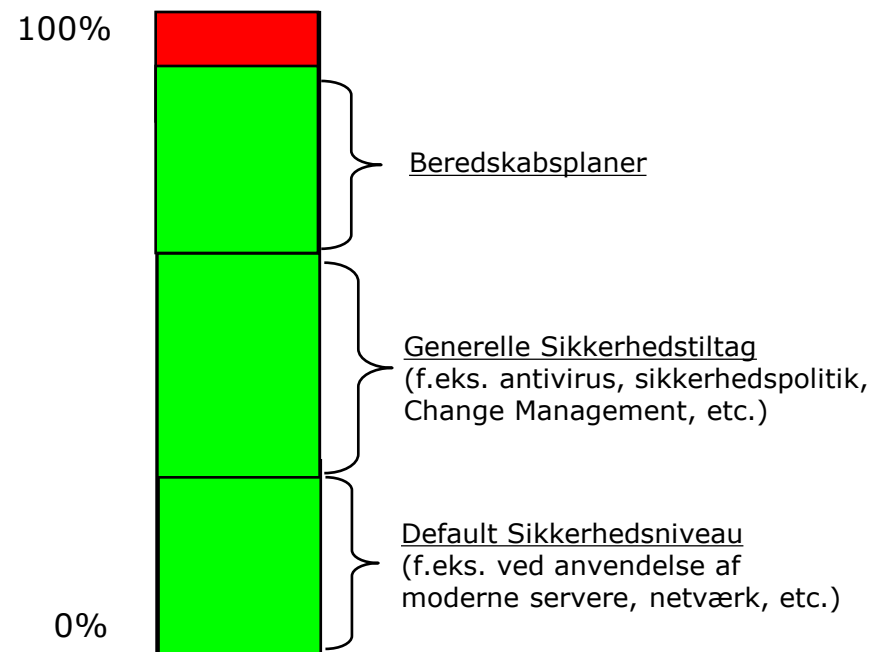
# Forretningsprocesser og beredskab



# Forretningsprocesser og beredskab



# HVORFOR er beredskab vigtigt?



Man kan aldrig sikre sig 100% mod nedbrud af længere varighed,  
men et beredskab vil øge paratheden til at håndtere situationer, som falder  
udenfor de almindelige driftsprocedurer.



# Risikovurdering og risikohåndtering

# Sikkerhedsmål

Hvordan vurderer man hvad der skal beskyttes, hvordan  
det skal beskyttes –  
og hvor mange ressourcer skal indsættes ?

# Risk ?





# Risikovurdering

- Risikovurdering er en proces der **identificere de risici** som kan påvirke IT ressourcerne eller organisationen som helhed.
- Risikovurderingen danner grundlaget for at kunne **prioritere** sikkerhedsindsatsen og besvarer spørgsmålene:
  - Bruger vi for få eller for mange ressourcer på sikkerhed?
  - Bruger vi de tilgængelige ressourcer bedst muligt?
- Risikovurderinger gennemføres **periodisk** (typisk årligt) samt ved **anskaffelse** af nye it-systemer eller større **ændringer** i organisationen, it-miljøet eller trusselsbilledet.

Undgår ting som "Er internettet sikkert?"



Det er svært for ledelsen at svare på:

"Hvad er den faktiske risiko, og hvad er de faktiske omkostninger eller andre konsekvenser ved et sikkerhedsbrud i min virksomhed?"

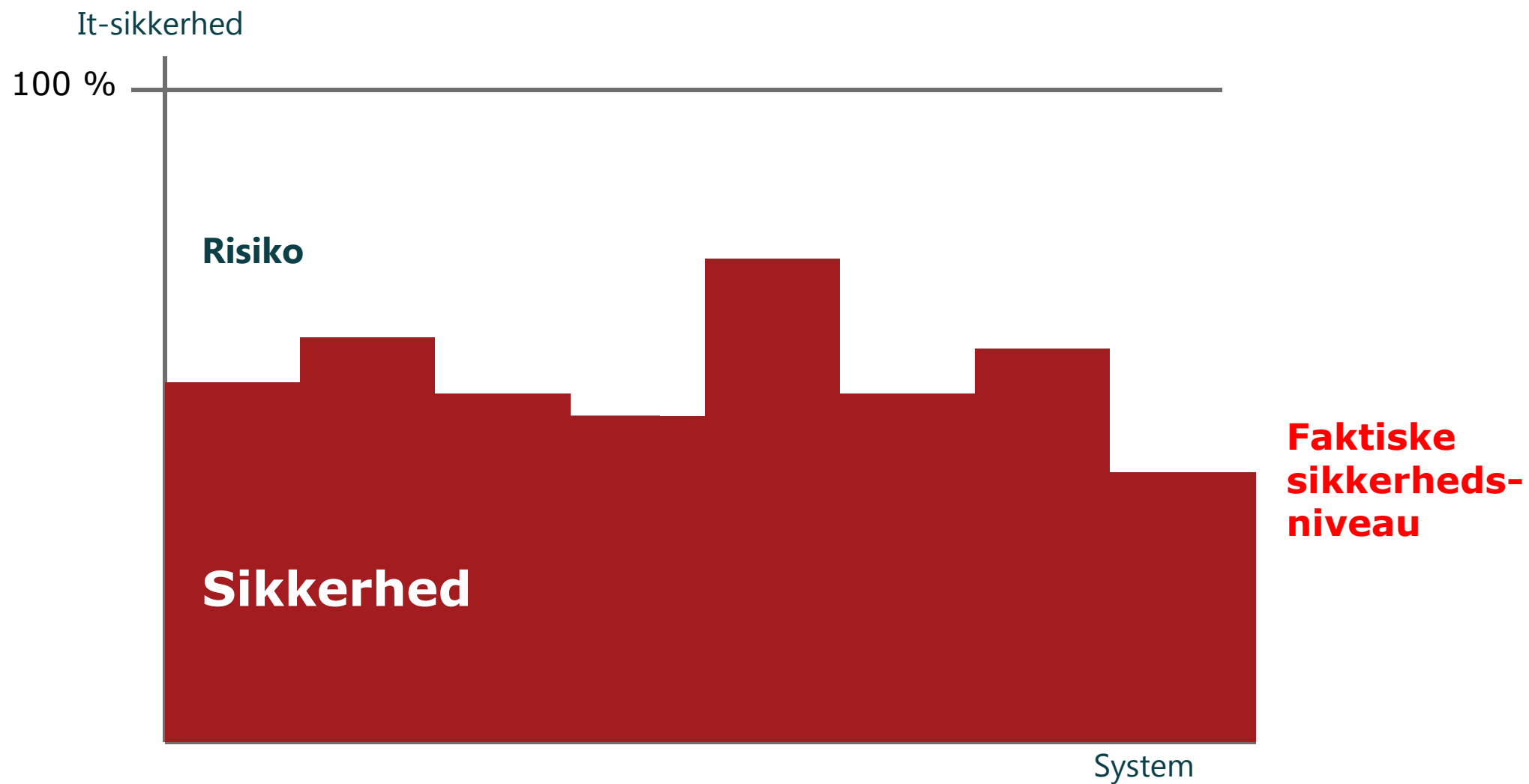


## Risikovurdering – aldrig 100% sikkerhed

“The only system which is truly secure is one which is switched off and unplugged, locked in a titanium lined safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards. Even then, I wouldn't stake my life on it.”

Gene Spafford

# Ønskede sikkerhedsniveau ?



# Different approaches to risk assessment

How do you identify relevant risks and threats?

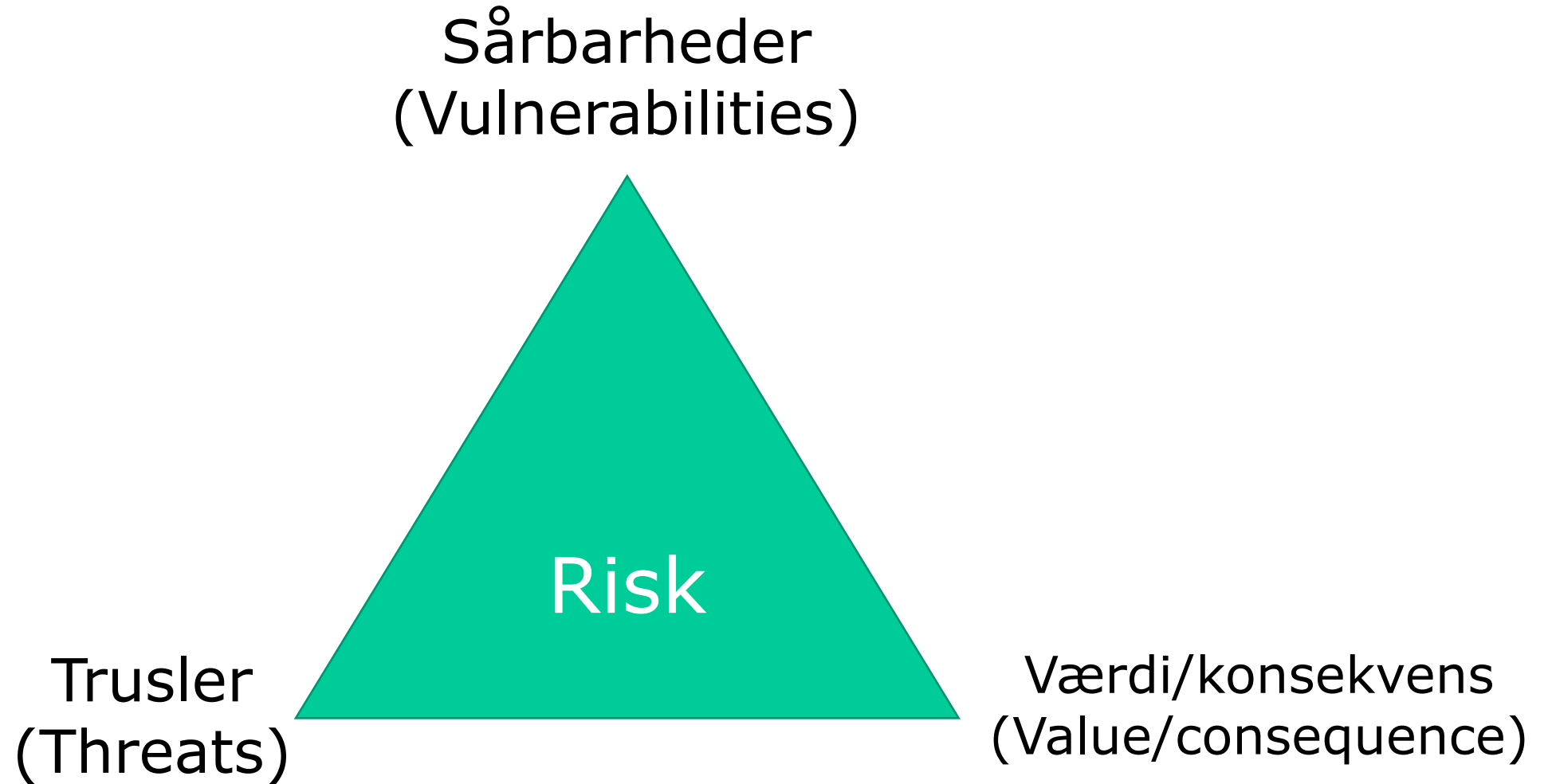
**Threat assessment**

**Risk modeling**

><

**Risk assessment**

# Risk assessment





# Risikovurdering – oversvømmelse af serverrum

**Trussel:** Oversvømmelse

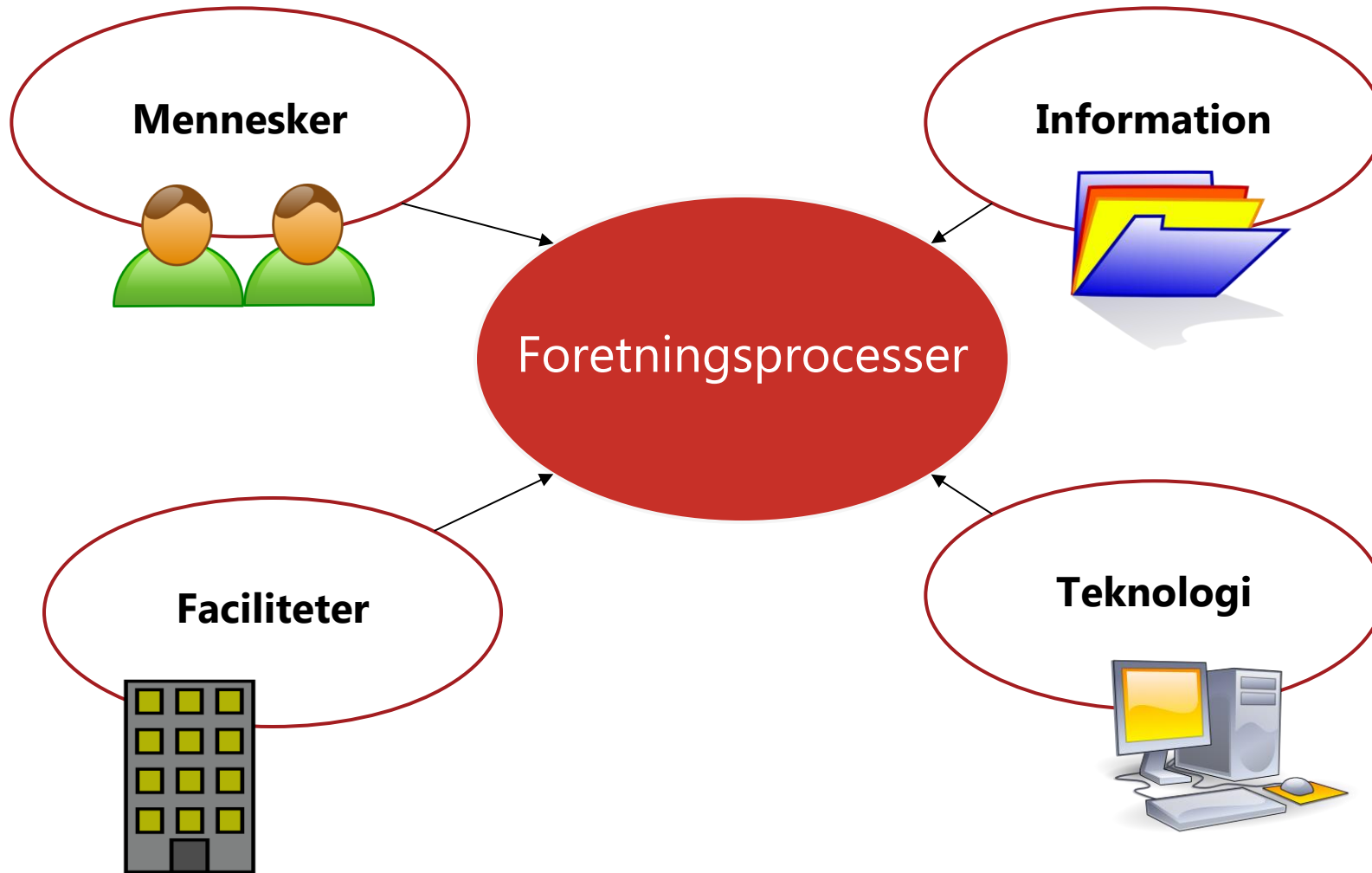
**Sårbarhed:** Serverrummet er i kælderen

**Sandsynlighed:** Erfaringen er, at vi får en oversvømmelse hver 20. år. Med de nuværende klimaforandringer forventer vi, at der vil komme oversvømmelser fra havnen hver 5. år

**Konsekvens:** Kælder oversvømmes og vand ødelægger derved servere

**Sikkerhedstiltag:** Flytning af serverrum til 3.sal kan fjerne sårbarhed. Alternativt outsource/cloud-source

# Typer af aktiver

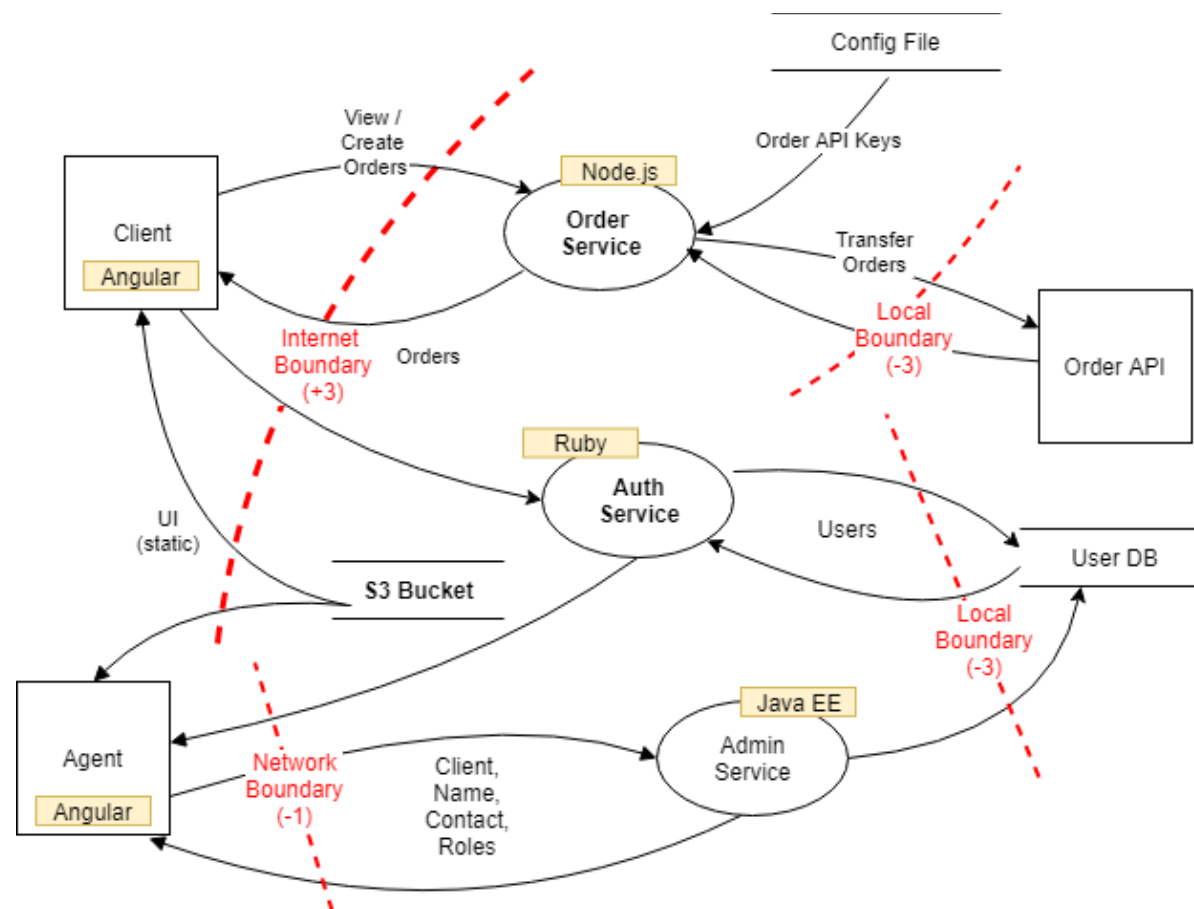


# STRIDE

The STRIDE threat model helps to answer, "what can go wrong in this system we're working on?"

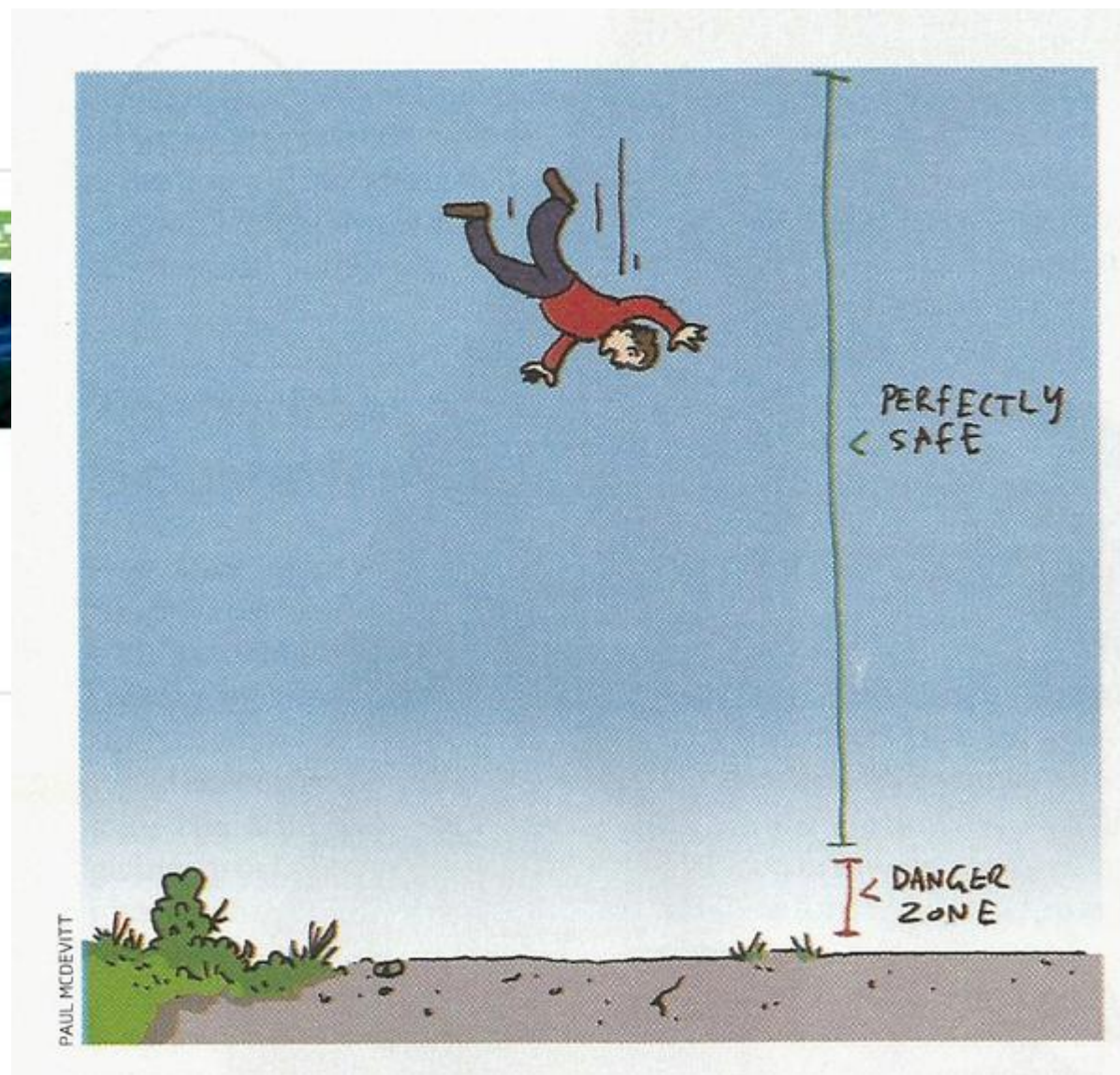
Threat	Desired property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiability
Information disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

# Trusselsidentifikation - så detaljeret som nødvendigt



STRIDE/DREAD, Attack Trees etc, etc  
Granular threat identification

# Det er svært at vurdere risikoen



ough

# Hvad skal risikovurderingen bruges til!

Trusselsvurderingen finder trusler

– samles i et risiko register

Nr.	Beskrivelse
1	Persondata i Dropbox
2	Server sårbarhed
3	Malware fører til datatab



# Hvad skal risikovurderingen bruges til!

Trusselsvurderingen finder trusler

– samles i et risiko register

Nr.	Beskrivelse	Sandsynlighed	Konsekvens
1	Persondata i Dropbox	Høj	Høj
2	Server sårbarhed	Mellem	Lav
3	Malware fører til datatab	Mellem	Mellem

# Risikovurdering

Trusler skal vurderes efter identifikation

- Teknisk risikovurdering
- Forretningsmæssig risikovurdering

# Forretningsmæssig risikoanalyse

Interview med ledere og forretningsansvarlige

Afdækning af konsekvenser:

Tab af indtægt, image tab, negativ omtale i pressen, mister mulighed for at opfylde kontrakter osv.

# Accepterer risiko

En risiko kan accepteres, hvis det vurderes, at risikoen er lav, eller at udgifterne til at implementere sikringsforanstaltninger ikke står mål med truslen.

Man skal ikke bruge flere penge på beskyttelse end værdien af de aktiver man skal beskytte.

## Eksempel

- Meteornedslag er katastrofale men sjældne
- Giver det mening at installere et meteorskjold?

# Ledelsesopmærksomhed og synlighed

Hvordan sikre man, at der bliver afsat ressourcer til sikkerhed?

Hvorfor skal "Projekt B" bruge 10% af budgettet på it-sikkerhed?

# Hvad skal risikovurderingen bruges til!

Risikovurderinger skal være et værktøj - de skal kunne bruges aktivt

Skal være klart og tydeligt visuelt:

- Kommunikerer risikobilledet
- Prioriterer aktiviteter

Vær klar på **hvorfor** du laver risikovurderingen !

(er det at finde sårbarheder, et ledelsesværktøj, sikre ressourcer...)



# Risikovurdering - simpel

No.	Threat	Risk
1.	Unencrypted data is stored on device. If device is stolen or otherwise lost data is readable and usable.	Low
	<i>Comments:</i> Encryption should be enabled by default on the devices. Confidential data is not stored on the device and cannot be accessed from the device.	
2.	Users will choose not to use access PINs or use weak PINs (“1234”). If device is lost or stolen, the device, apps and all data can be accessed.	Medium
	<i>Comments:</i> Authentication requirements should be applied through policies and device management solutions, or through user awareness (less effective). However the data that can be accessed on the device is not Confidential.	

Farver bruges til at gøre potentiel risiko tydelig

# Indhold af del-analyser

## System og data klassifikation

F.eks.	Kritisk
	Mindre kritisk
	Ikke kritisk
	Ikke relevant

# Simpel risikoanalyse

$$\text{Risiko} = \text{Sandsynlighed} \times \text{Konsekvens}$$

Sandsynlighed kan kategoriseres som:

Meget Sandsynlig	(4)
Sandsynlig	(3)
Mindre Sandsynlig	(2)
Ikke sandsynlig	(1)

Konsekvens kan kategoriseres som:

Katastrofal	(4)
Kritisk	(3)
Skadelig	(2)
Uskadelig	(1)

# Risiko Matrix

Meget sandsynlig	4	8	12	16
Sandsynlig	3	6	9	12
Mindre sandsynlig	2	4	6	8
Ikke sandsynlig	1	2	3	4

	No/low consequence	Medium consequence	High consequence
No/low probability	1x1=1	1x2=2	1x3=3
Medium Probability	2x1=2	2x2=4	2x3=6
High probability	3x1=3	3x2=6	3x3=9

Low/no risk	
Medium risk	
High risk	

# Risikovurdering - applikation

No.	Threat	Likelihood	Consequence	Risk
1.	Unencrypted data is stored on device. If device is stolen or otherwise lost data is readable and usable.	No	High	Low
	<i>Comments:</i>	Encryption should be enabled by default on the devices. Confidential data is not stored on the device and cannot be accessed from the device.		
2.	Users will choose not to use access PINs or use weak PINs ("1234"). If device is lost or stolen, the device, apps and all data can be accessed.	High	Low	Medium
	<i>Comments:</i>	Authentication requirements should be applied through policies and device management solutions, or through user awareness (less effective). However the data that can be		

# Risikovurdering – eksempel

Microsoft Excel - F-Dept.xls

File Edit View Insert Format Tools Data Window Help

Type a question for help

85%

A1 B C D E F G H I J K

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33

**1. Forretningsmæssig risikovurdering for telefoni og omstilling** [\[retur til oversigt\]](#)

**Fortrolighed**

I hvilken grad medfører manglende fortrolighed	Vurdering	Kommentarer
a. Tab af konkurrence mæssige fordele ?	Uskadelig	ej aktuelt
b. Risiko for økonomiske tab ?	Kritisk	Store afledte omkostninger til spinhåndtering
c. At det offentlige omdømme påvirkes ?	Skadelig	Medarbejdere forventer at kunne drøfte interne og fortrolige anliggender telefonisk uden risiko for fortrolighedsbrud
d. Yderligere omkostninger ?	Uskadelig	
e. At lovmæssige krav ikke kan opfyldes ?	Uskadelig	

**Integritet**

I hvilken grad medfører manglende integritet (pålidelighed af data):	Vurdering:	Kommentarer
a. At beslutninger ikke kan træffes tilfredsstillende ?	Skadelig	Informationsindhentning og koordination kan blive vanskeliggjort
b. Risiko for svig ?	Uskadelig	Næppe
c. At de daglige opgaver ikke kan gennemføres ?	Kritisk	E.g. hvis nummer-databasen korrumpes vil man ikke kunne ringe og videregive korrekt internt
d. At det offentlige omdømme påvirkes ?	Skadelig	Negativ medieomtale mv.
e. Medføre yderligere omkostninger ?	Skadelig	Oprydning og omkonfigurering, samt evt. problemer ifht. håndtering af frister
f. At lovmæssige krav ikke kan opfyldes ?	Skadelig	Igangværende opgaver kan påvirkes

**Tilgængelighed**

Efter hvor lang tid medfører manglende tilgængelighed:	Ved nedbrud under 1 time	Ved nedbrud mellem 1 time og 8 timer	Ved nedbrud mellem 8 timer og 1 døgn	Ved nedbrud mellem 1 døgn og 2 døgn	Ved nedbrud over 2 døgn	Er der tidspunkter hvor nedbrud er særligt kritisk ?
a. At nødvendige beslutninger ikke kan træffes tilfredsstillende?	Skadelig	Kritisk	Kritisk	Katastrofalt	Katastrofalt	
b. Øgede omkostninger?	Uskadelig	Skadelig	Skadelig	Kritisk	Katastrofalt	
c. Mistet indtægt ?	Uskadelig	Uskadelig	Uskadelig	Uskadelig	Uskadelig	
d. At forpligtelser ikke kan opfyldes?	Skadelig	Kritisk	Kritisk	Katastrofalt	Katastrofalt	
e. At det offentlige omdømme påvirkes?	Skadelig	Kritisk	Kritisk	Kritisk	Katastrofalt	
f. At lovmæssige krav ikke kan opfyldes?	Skadelig	Kritisk	Kritisk	Katastrofalt	Katastrofalt	

**Vejledning til overordnet risikovurdering:**

I vurderingsfeltet angives et niveau:

1 - Katastrofalt  
2 - Kritisk  
3 - Skadelig  
4 - Uskadelig

Hvis vurderingen udfyldes elektronisk er der "pull-down" kasser til dette formål i vurderingscellerne.

Når man udfylder tilgængelighedsværdierne foregår dette på samme måde.

Katastrofalt  
Kritisk  
Skadelig  
Uskadelig

1 2 3 4 5 6 7 8 9 10 11

Ready NUM



Microsoft Excel - T-Server drift-risikovurdering.XLS

File Edit View Insert Format Tools Data Window Help

Type a question for help

E3

fx

A B C D E F G H I J K

1

2

3

4

Indsættelinie for det markerede

Ole til linie

Skema til it-risikovurdering, Serverdrift & klientmiljø

Vil den nye ansættelse implementering eller ændring kunne medføre

Sandsynlighed (5) for at truslen indtræffer

Konsekvenser

Konsekvens (1)

Kalibreret vægter risiko

Kan vi acceptere nuværende situation

Noter

Forslag til tekniske eller administrative tiltag til at imødegå risikoen

5

6

7

8

9

10

11

12

13

Bugene

At der sker misbrug af anden brugers systemadgang, f.eks. ved gæt af kodeord, misbrug af udstyr der er loggeret på.

At en ansat laver uautoriserede ændringer af data

At en ansat klassificerer data forkert

En ansat udøver sabotage, f.eks. sletter vitale data

At en ansat får uretmæssig adgang til data

At en ansat omgår sikkerheden

At der sker tyveri af interne data / software

At der ikke er den nødvendige funktionsadskillelse til at imødegå svig og misbrug

At tredjeparts personale (samarbejdspartner, konsulent, leverandør) misbruger systemer eller data

Sandsynlig

Mindre sandsynlig

Meget sandsynlig

Mindre sandsynlig

Sandsynlig

Meget sandsynlig

Mindre sandsynlig

Sandsynlig

Fortrolighed, tilgængelighed og pålidelighed af data kompromitteres

Tilgængelighed og pålidelighed kompromitteres

At data ikke behandles i overensstemmelse med deres væsentlighed - brud på fortrolighed, tilgængelighed og pålidelighed.

Brud på fortrolighed, tilgængelighed og pålidelighed.

Brud på fortrolighed, tilgængelighed og pålidelighed.

Brud på fortrolighed, tilgængelighed og pålidelighed.

Brud på fortrolighed, tilgængelighed og pålidelighed.

Brud på pålidelighed.

Skadelig

Skadelig

Skadelig

Kritisk

Skadelig

Skadelig

Skadelig

Skadelig

Middel

Lav

Middel

Middel

Middel

Middel

Lav

Middel

Nej

Ja

Ja

Ja

Ja

Nej

Ja

Ja

Sløseri med password og gule sedler. Skærmlås.

Navision superbrugere kan slette.

Der kan være eksterne kontakter i en distributionsliste på mailsystemet som man tror er intern.

I relation til brug af andres password til f.eks. Navision ved f.eks. fravær

Formalia er på plads, men implementering ifht. JyskeBank halter. Derudover har flere adgang til andres navision password ifv. gule sedler.

Eksterne er i visse tilfælde oprettet i miljøet og på distributionslister i

Der bør være skærmlås med 10-15 min. låsetid - særligt på it-personale der har administrative adgange fra desktop og remote-stationer. Indskærp forhold ifht. brug af password på gule sedler.

I) Etabler sikkerhedsmæssig checkliste for ansættelser der indebærer admin-privilegier. II) Etabler checkliste og risikovurderingsskabelon for fratrædelse af nøglemedarbejdere.

Opret yderligere brugeradgange hvis behovet er til stede. Sporbareheden skal være på plads og alternativt må opgaven vente på at nøglepersonen er tilgængelig.

Underskrift og tiltrædelse af it-sikkerhedspolitik inden adgange tildeles!

Vejledning til it-risiko

NB: Gå til fanen 'Vejledning procedure/vejledning.

I) Bekræft at relevante yderligere trusler og

II) Vurder sandsynlig indtræffer

III) Beskriv konsekvenser

IV) Vurder konsekvenser

V) Skitser evt. i noter eksisterer i organisationen laves linieskift inden

Vejledning Risikovurdering

NUM

# Vurdering og prioritering

- Anbefal handlinger (f.eks. mitigation/compensation)
- Vurder hvordan det hjælper, giver det værdi, hvordan hjælper anbefalingen egentlig
- Hvis handling ikke hjælper – find noget andet der gør

B	C	D	E	F	G	H	I
<b>Risk Mitigation Action Plan for [INSERT NAME OF APPLICATION]</b>							
Issue number and Risk description	Mitigating Action	Priority	Raised (date)	Approved by SO (Date)	Expected go live date	Responsible	Next step and comments

# Case – ledelsesrapportering

DIKUcorp er en medievirksomhed med en årlig omsætning på 100 mio DKR. Virksomhedens webserver har en kendt RCE (Remote Code Execution) sårbarhed i virksomhedens CMS, der vil kunne udnyttes til at tage fuld control over serveren.

En opdatering har været tilgængelig i 18 måneder men er endnu ikke rullet ud fordi virksomheden normalt venter til leverandøren har en samlet sevicepack opdatering klar.

Virksomhedens webshop, der står for omkring 80% af virksomhedens omsætning, ligger på serveren. Der ligger en række databaser på serveren, flere indeholder persondata om virksomhedens 800.000 kunder.

## **Risikovurdering:**

# Case – ledelsesrapportering

DIKUcorp er en medievirksomhed med en årlig omsætning på 100 mio DKR. Virksomhedens webserver har **en kendt** RCE (Remote Code Execution) sårbarhed i virksomhedens CMS, der vil kunne udnyttes til at **tage fuld control** over serveren.

En opdatering har været tilgængelig i 18 måneder men er endnu ikke rullet ud fordi virksomheden normalt venter til leverandøren har en samlet sevicepack opdatering klar.

Virksomhedens webshop, der står for omkring 80% af virksomhedens omsætning, ligger på serveren. Der ligger en række databaser på serveren, flere indeholder persondata om virksomhedens 800.000 kunder.

## Risikovurdering:

Description	Likelihood	Consequence	Risk	Notes
RCE i CMS	High	High	High	Sikkerhedspatch 2018-A6763G bør installeres

# Ledelseskommunikation

DIKUcorp er en medievirksomhed med en årlig omsætning på 100 mio DKR. Virksomhedens webserver har **en kendt** RCE (Remote Code Execution) sårbarhed i virksomhedens CMS, der vil kunne udnyttes til at **tage fuld control** over serveren.

En opdatering har været tilgængelig i 18 måneder men er endnu ikke rullet ud fordi virksomheden normalt venter til leverandøren har en samlet sevicepack opdatering klar.

Virksomhedens webshop, der står for omkring 80% af virksomhedens omsætning, ligger på serveren. Der ligger en række databaser på serveren, flere indeholder persondata om virksomhedens 800.000 kunder.

## Ledelseskommunikation: Hvad siger du?

“Vi har en RCE i vores CMS, jeg skal bruge 1 mio til at teste og installere et sikkerhedspatch og forbedre sikkerheden generelt”

Description	Likelihood	Consequence	Risk	Notes
RCE i CMS	High	High	High	Sikkerhedspatch 2018-A6763G bør installeres

# Ledelseskommunikation

Hvad tænker lederen?

**Jeg har 1 mio i budgettet, skal jeg bruge den på**

- a) Forretningsudvikling - businesscase forventer 3% øget salg
- b) Energibesparelser, nedbrug strømforbrug, forventet besparelse 0,6%
- c) "Sikkerhedspatch til RCE i CMS" - et eller andet med hjemmesiden

# Ledelseskommunikation

DIKUcorp er en medievirksomhed med en årlig omsætning på 100 mio DKR. Virksomhedens webserver har en kendt RCE (Remote Code Execution) sårbarhed i virksomhedens CMS, der vil kunne udnyttes til at tage fuld control over serveren.

En opdatering har været tilgængelig i 18 måneder men er endnu ikke rullet ud fordi virksomheden venter til leverandøren har en samlet sevicepack opdatering klar.

Virksomhedens webshop, der står for omkring **80% af virksomhedens omsætning**, ligger på serveren. Der ligger en række databaser på serveren, flere indeholder **persondata om virksomhedens 800.000 kunder**.

Description	Likelihood	Consequence	Risk	Notes
RCE i CMS	High	High	High	Sikkerhedspatch 2018-A6763G bør installeres



# Eksempel på konsekvensoversigt

Konsekvens	Kunder	Image	Aktiekurs <sup>1</sup>	Personale Ressource-belastning	Personale Tiltrække nye medarbejdere	Interessenter Offentlige og kontrollerende	Interessenter Samarbejds-partnere	Økonomisk
<b>Uskadelig</b>	Mister under 10 privatkunder	Ingen offentlig omtale	Aktiekursen falder ikke	Under en uges ekstraarbejde	Ingen påvirkning	Ingen påvirkning	Ingen påvirkning	Direkte økonomisk tab under 100 t. kr.
<b>Skadelig</b>	Mister under 500 privatkunder / 5 store virksomheder	Historie i dagblad eller i TV nyheder. Forsiden Børsen	Aktiekursen falder 0-2 %	Under 2 mandeår i ekstra arbejde	Ingen væsentlig påvirkning	Væsentlig påtale eller advarsel fra myndigheder	Samarbejdspartnere ønsker sikkerhed for fortsatte leverancer.	Tab mellem 100 tkr og 10 mio. kr. , svarer til forøgelse af udgifter på under 1%
<b>Kritisk</b>	Mister under 1.000 privatkunder eller 10 store virksomheder	Forsiden af dagblade og hovedhistorie i TV	Aktiekursen falder 2-10 %	Under 10 mandeår i ekstraarbejde	Medarbejdere	Sat under	Partnere fornyer	Tab mellem 10 og
<b>Katastrofalt</b>	Mister mere end 1.000 privatkunder eller mere end 10 store virksomheder	Forsiden af landsdækkende avis eller hovedhistorie i landsdækkende TV i en længere periode	Aktiekursen falder med 10+ point	Mere end 10 mandeår i ekstraarbejde				

rigtige niveau ??

- "Høj" sikkerhed
- "Lav" sikkerhed
- "Best practice"

Det er  
forretningen og  
lovgivningen der  
stiller krav til  
sikkerhedsniveau



Konsekvenstype	Politisk/Strategisk	Økonomisk	Administrativ/proces mæssig	Omdømme	Forhold til interessenter	Menneskelige	Privacy	Brud på lovgivningen	Samfundsmæssige risici		Ledelsens risikoappetit (årligt)
	Medfører indskrænkninger i evnen til at handle i en periode	Medfører meromkostninger eller tab	Medfører administrative belastninger	Påvirker omdømme i uønsket retning	Påvirker forholdet til interessenter	Medfører konsekvenser for det enkelte individ	Medfører brud på privacy	Medfører brud på lovgivning, fx forvaltningslov og straffelov			
<b>4. Graverende/ødelæggende (uacceptabelt)</b>	Ministeren må gå af. Bliver ude af stand til at gennemføres vigtige aktiviteter, som er planlagt i en periode fremover	Vesentlige økonomiske tab. Bliver sat under administration	Administrative ressourcer må udvides urealistisk	Vesentlig skade på omdømme. Ministeren må gå af	Vesentligt nedbrud i det generelle samarbejde med interessenter	Menneskeliv står på spil	Den enkelte udsættes for uacceptable krænkelse af privatlivet. Der træffes bebyrdende afgørelser mod den enkelte på et forkert grundlag. Store mængder følsomme data videregives uretmæssigt	Kritisk lovgivning, fx straffeloven brydes. Ministeren må gå af.	Alvorlig fare for borgeres sikkerhed		0 hændelser
<b>3. Meget alvorlig (kritisk)</b>	Medfører revurdering af vigtige aktiviteter på kort sigt	Store økonomiske tab med risiko for at blive sat under administration	Der må trækkes væsentligt på eksisterende og nye administrative ressourcer	Offentligheden fatter generel negativ interesse mod organisationen	Generelt forringet samarbejde med interessenter	Alvorlig personskade	Den enkelte fratages råderetten over egne data. Enkelte følsomme data videregives uretmæssigt	Lovbrud, der er kritiske og kan stille ministeriet i miskredit	Større læk af borgeres personlige oplysninger		Max 1 hændelse
<b>2. Mindre alvorlig</b>	Planlagte aktiviteter kan gennemføres med mindre justeringer	Meromkostninger og tab i begrænset niveau, som kan kræve mindre budgetændringer	Håndteres inden for rimeligt ekstra administrativt ressourcetræk	Forbigående opmærksomhed fra enkelte grupper	Foringet samarbejde med interessenter i enkeltsager	Den enkelte udsættes for gener, men ikke noget alvorligt	Der er formelle mangler i de oplysninger, der gives den enkelte, men ikke i graverende grad. Ikke-følsomme data videregives uretmæssigt	Manglende overholdelse af administrative procedurer og regler, som ikke er af kritisk karakter	Mindre læk af borgeres personlige oplysninger		<10 hændelser
<b>1. Ubetydelig (uvæsentlig)</b>	Ingen særlig påvirkning	Ingen særlig påvirkning	Håndteres uden særligt ressourcetræk i de administrative funktioner	Ingen særlig påvirkning	Ingen særlig påvirkning	Ingen særlig påvirkning	Ingen særlig påvirkning	Ingen særlig påvirkning	Ingen særlig påvirkning		<20 hændelser

# Ledelseskommunikation





# Opsummering

IT-sikkerhedsledelse, incl. risikovurderinger, er en kritisk del af it-sikkerheden – og **et meget stærkt redskab**



# Awareness – sikkerhedskultur og adfærdsdesign

# Adfærdsdesign i awareness-arbejdet



Den enkelte medarbejders adfærd er afgørende for hele organisationens informationssikkerhed

Derfor er det vigtigt at styrke medarbejdernes forståelse af deres ansvar i organisationens informationssikkerhed

**“Den menneskelige firewall”**

**Men viden er ikke nok.**

**Der skal adfærdsforandring til, før der kan opstå en stærk sikkerhedskultur.**



# Grundlaget er viden om sikkerhed

Awareness-arbejdet starter med, at **budskaber og målgrupper defineres**.  
Man kan ikke forvente sikkerhed uden at have informeret medarbejderne



Håndtering af attachments



USB-nøgler



Stærke kodeord



Udviklingsafdelingen



HR-medarbejdere og jurister

Forarbejdet skal baseres på viden om, hvordan medarbejderne arbejder i dag:  
Brug risikovurderinger, globale trusler som ransomware eller phishing, triggers i dagligdagen  
(i hvilke situationer kan der opstå brud på sikkerheden) osv.

Materialet skal være **relevant for modtageren**. Hvis det er for generisk eller irrelevant for medarbejderne, mister man deres opmærksomhed.

# Sikkerhedspakken – der er mange forskellige metoder

Folder

Plakater

Film

Musemåtter

Information på intranettet

Artikler i firma bladet

Møder

Undervisning

Emails

Skærmskånere

Phishing angreb

Efterladte USB-nøgler

Social engineering



# Sikkerhedspakken samlet



Mange awareness-kampagner standser forarbejdet her og går direkte til produktion.

Men efter budskaber og målgrupper er defineret, og det første overblik over forskellige teknikker fra plakater til udsendelse af e-mails er etableret, er det kritisk, at **budskaberne leveres effektivt.**

## Kommunikationsstrategi og plan

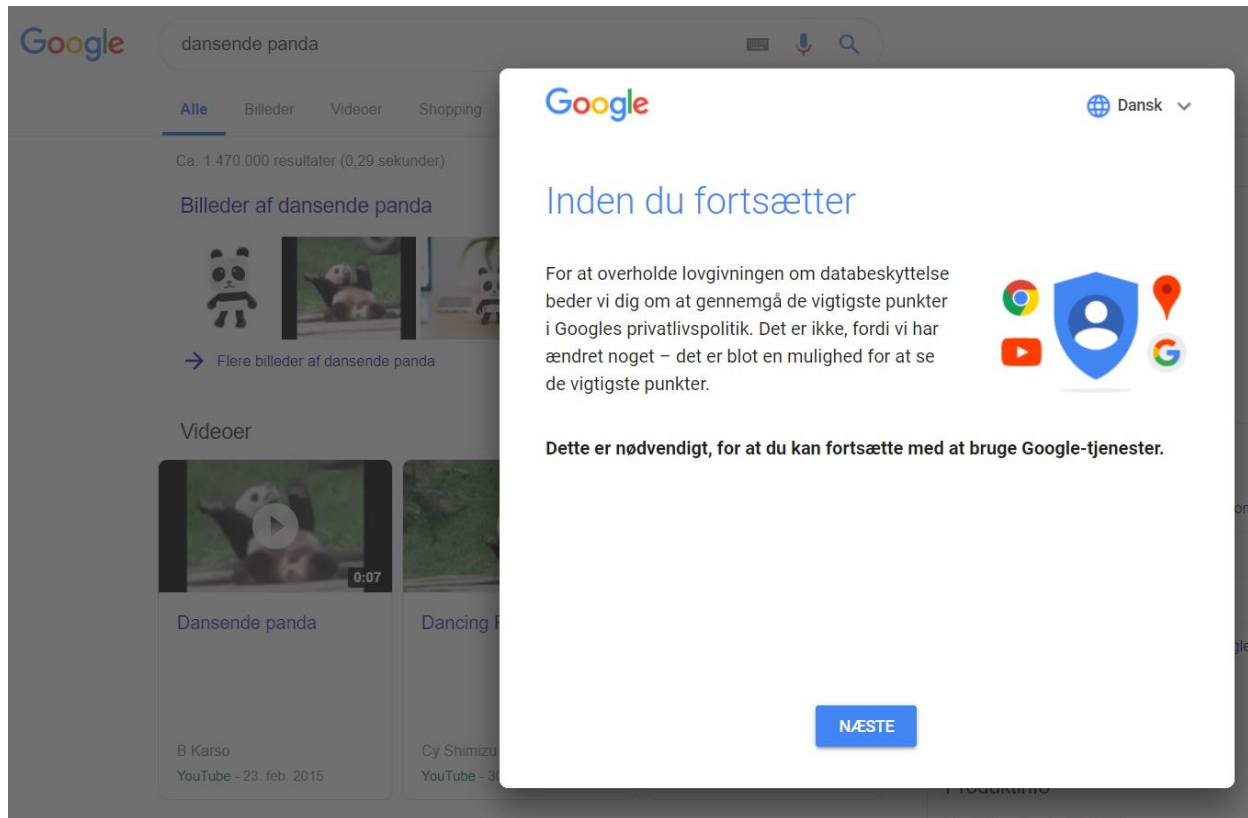
Målgrupper

Folder

E-læring

Opfølgning

# Brugerens mentale model



Overførslen af viden er kun effektiv, når modtagerne er **fokuseret** på det, der sker

Det vil sige, at budskaberne skal leveres i en situation, hvor medarbejderne er opmærksomme på sikkerheds-budskaberne

Mentalt må indlærings-situationen ikke være noget, der *skal overstås*, inden de kan komme videre til deres primære formål

# Sikkerhedsformlen



# Når mennesker træffer beslutninger



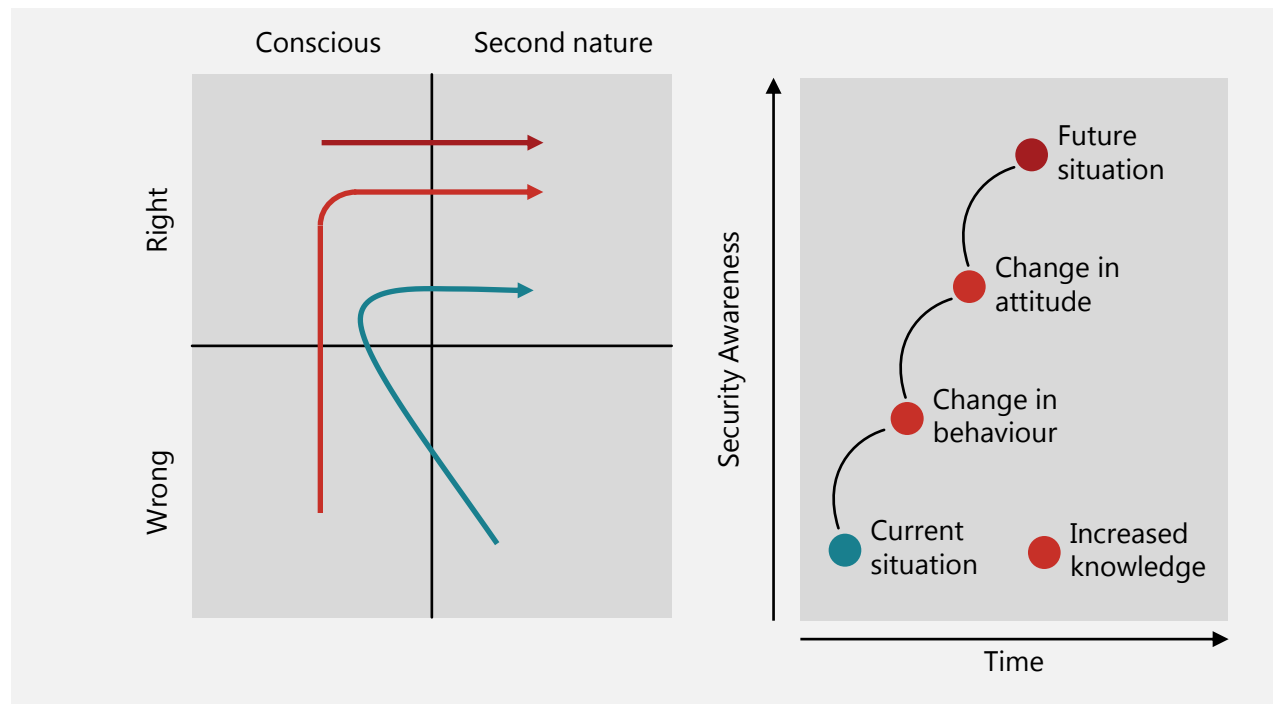
Daniel Kahneman beskriver i "At tænke – hurtigt og langsomt", hvordan, hvorfor og hvornår mennesker træffer beslutninger.

Kahnemans **system 1 og system 2**-model forklarer, hvorfor vi nogle gange handler forkert, selvom vi ved, det er forkert. System 1 handler hurtigt og instinktivt på trigger-hændelsen, inden system 2 når at reagere.

For at forbedre vores beslutninger fra ubevidste og forkerte skal sikkerheden gøres til naturlige handlinger gennem mere træning (beslutninger flyttes fra system 2 til system 1).



# Sikkerhed som naturlige handlinger



Sikkerhed kan flyttes fra system 2 til system 1 gennem **opfølgende træning**, der naturligvis stadig skal være relevant for modtageren, og stadig gives i situationer, hvor sikkerhed er det primære fokus.

# Ændringer

Awareness er en løbende aktivitet,  
det er ikke en engangsopgave

Skift medier og budskab for at undgå  
blindhed

Ansvar for sikkerhedsaktiviteter skal  
placeres hos de udførende



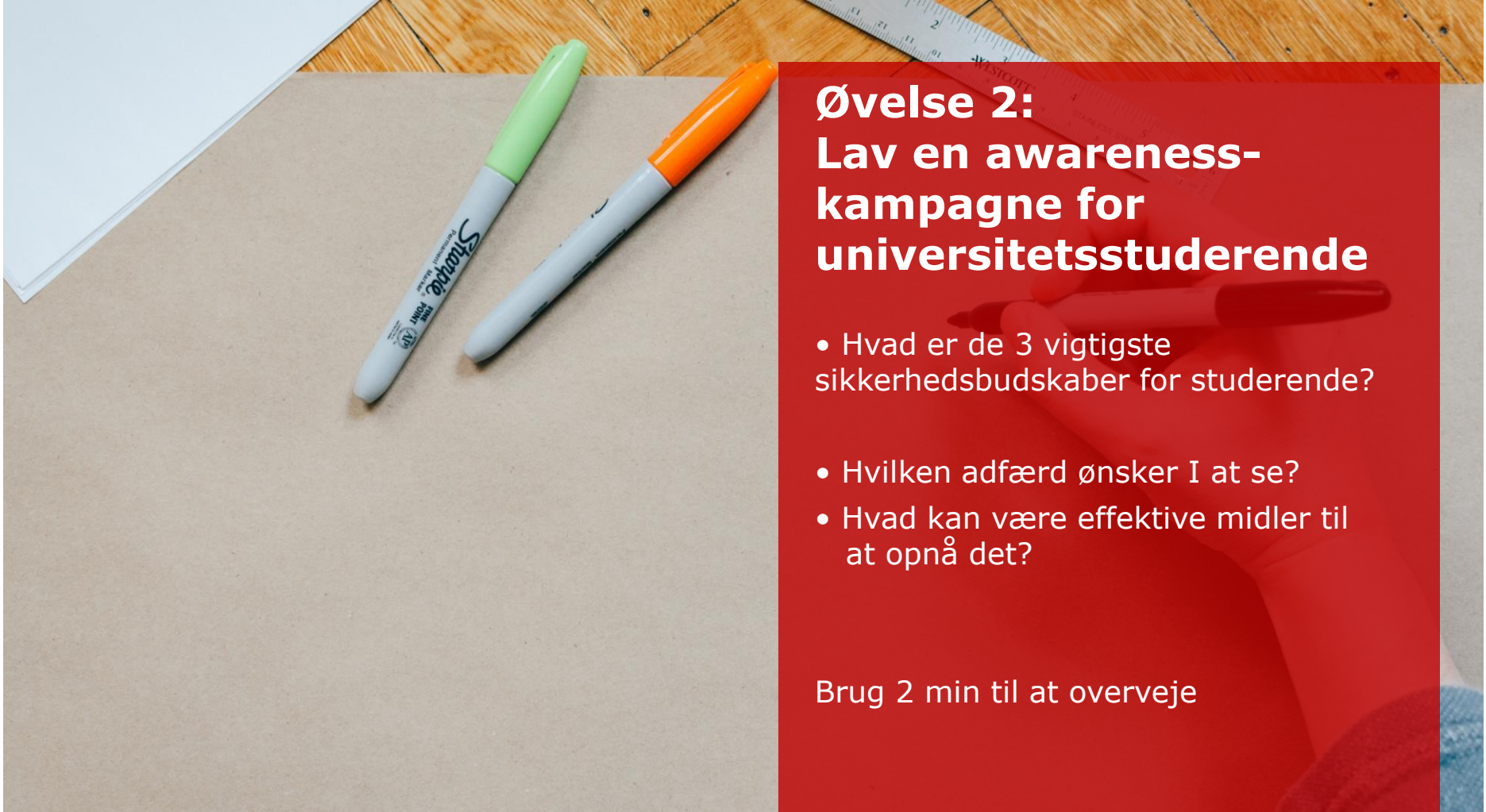
# Sikkerhed som naturlige handlinger



Konsekvens (positiv, men også negativ) og reinforcement er vigtige redskaber for hurtigt at træne system 1.

Derfor er fx phishingkampagner effektive i denne fase. Det viser medarbejderne konsekvensen af deres handlinger, så system 1 hurtigt lærer at handle rigtigt.

Information præcis på det tidspunkt, man skal til at udføre en potentielt usikker handling, kan fx også være effektiv i denne fase.

The background of the slide is a photograph of a workspace. It shows a wooden table surface with a piece of brown cardboard and a white sheet of paper. Two Sharpie markers, one green and one orange, are lying on the cardboard. A metal ruler is partially visible in the upper right corner. A red semi-transparent box is overlaid on the right side of the image, containing the text for the exercise.

## Øvelse 2: Lav en awareness- kampagne for universitetsstuderende

- Hvad er de 3 vigtigste sikkerhedsbudskaber for studerende?
- Hvilken adfærd ønsker I at se?
- Hvad kan være effektive midler til at opnå det?

Brug 2 min til at overveje





# The next lectures

- Sep 22: Malicious software
- Sep 26: Software security
- Sep 29: Security architecture (perimeter, zero trust, OT),  
Hardware security
- Oct 3: AI-security, Cloud-security, IoT-security...
- Oct 6: Intrusion detection, Network attacks
- Oct 10: Forensics
- Oct 20: Privacy, Data protection
- Oct 24: Privacy engineering, Privacy by design, PETS and GDPR

# Spørgsmål

