Cyber-forsikring til hvilken pris?

Hva betyr cyber-sikkerhet og cyber-risiko i kroner og øre?

Bjørnar Solhaug

Seminar om kost-nytte-analyse i en risikoevaluering

SINTEF, 18. februar, 2015

Cyberspace er overalt

- "Alle" bruker det
  - Myndigheter
  - Bedrifter
  - Privatpersoner
- Det brukes til "alt"
  - Offentlige tjenester
  - Økonomi
  - Underholdning
  - Sosialt
  - Handel
  - …

Cyber-risiko er overalt

Millioner av servere verden rundt har sårbarheten som gjør det relativt enkelt for uvedkommende å lese minnet deres.

Tekno Internett

«Hjerteblødning» rammer internett

Hackere kan ha forsynt seg i to år uten å etterlate seg spor. - **Svært alvorlig, mener Nasjonal Sikkerhetsmyndighet.**

Eksperter identitetsty

** Stadig flere forsø

** - Tra

50 nor for dat

Eit kraftig og avar

energibransjen. N

om at dei må vere på vakt.

Nyhe

I dag

nettsider var de siste

Heljar Ha

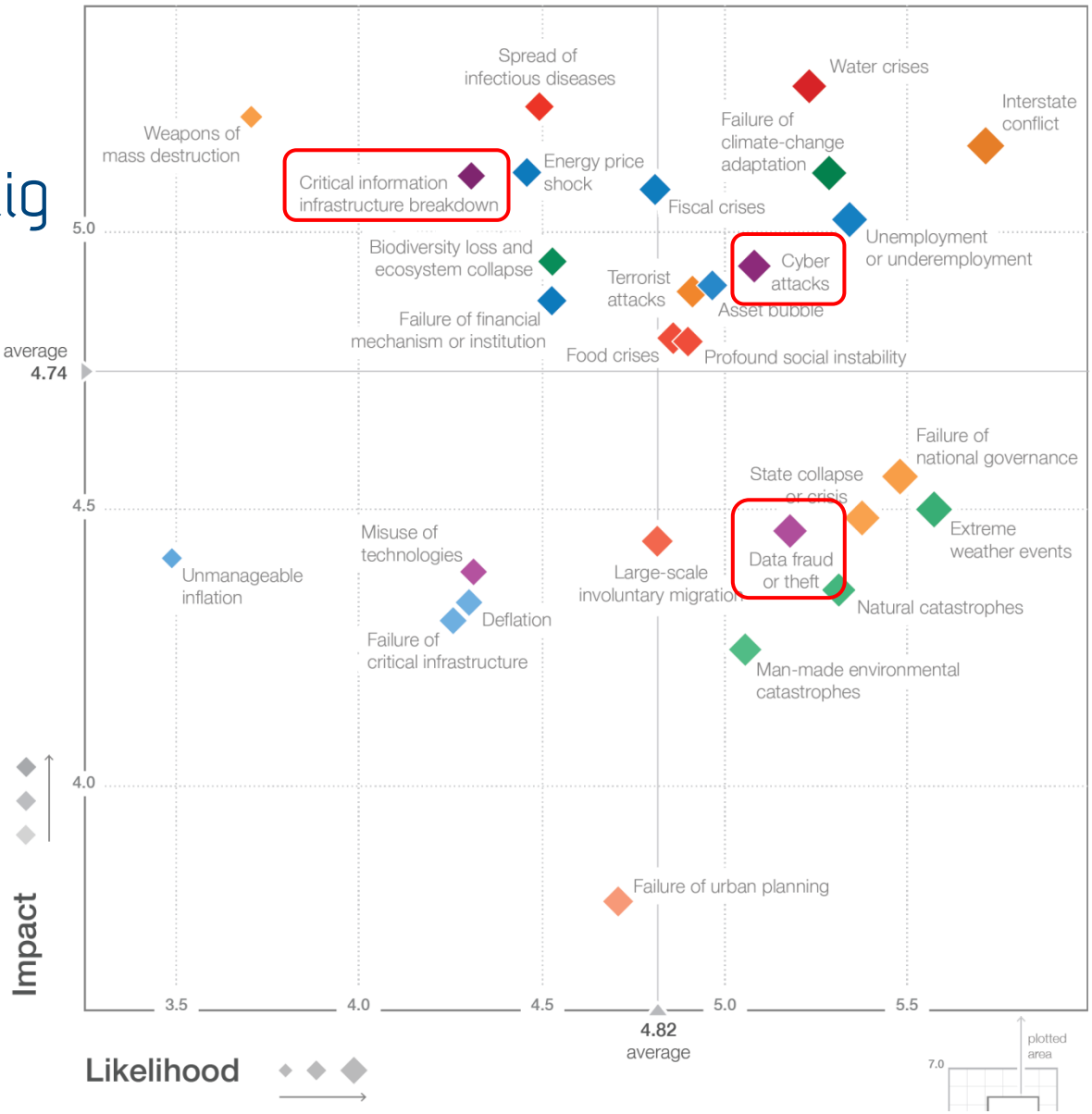
Publisert:

Norges Bank bekrefter a

Cyber-risiko er betydelig

- Cyber attacks
- Critical information infrastructure breakdown
- Data fraud or theft

World Economic Forum:
Global Risks 2015



Hvordan håndtere cyber-risiko?

- Tradisjonelt håndterer bedrifter sikkerhetsrisiko ved å etablere rutiner for sikkerhetsstyring og å investere i sikkerhetsmekanismer
- Cyber-risikoer kan imidlertid være vanskelig å vurdere og håndtere
  - Hva er truslene?
  - Hva er sårbarhetene?
  - Hva er konsekvensene?
  - Hva er sannsynligheten?
- Cyber-forsikring kan være et alternativ
  - Overføre risiko til tredjepart
  - Redusere usikkerhet

Cyber-forsikring til hvilken pris?

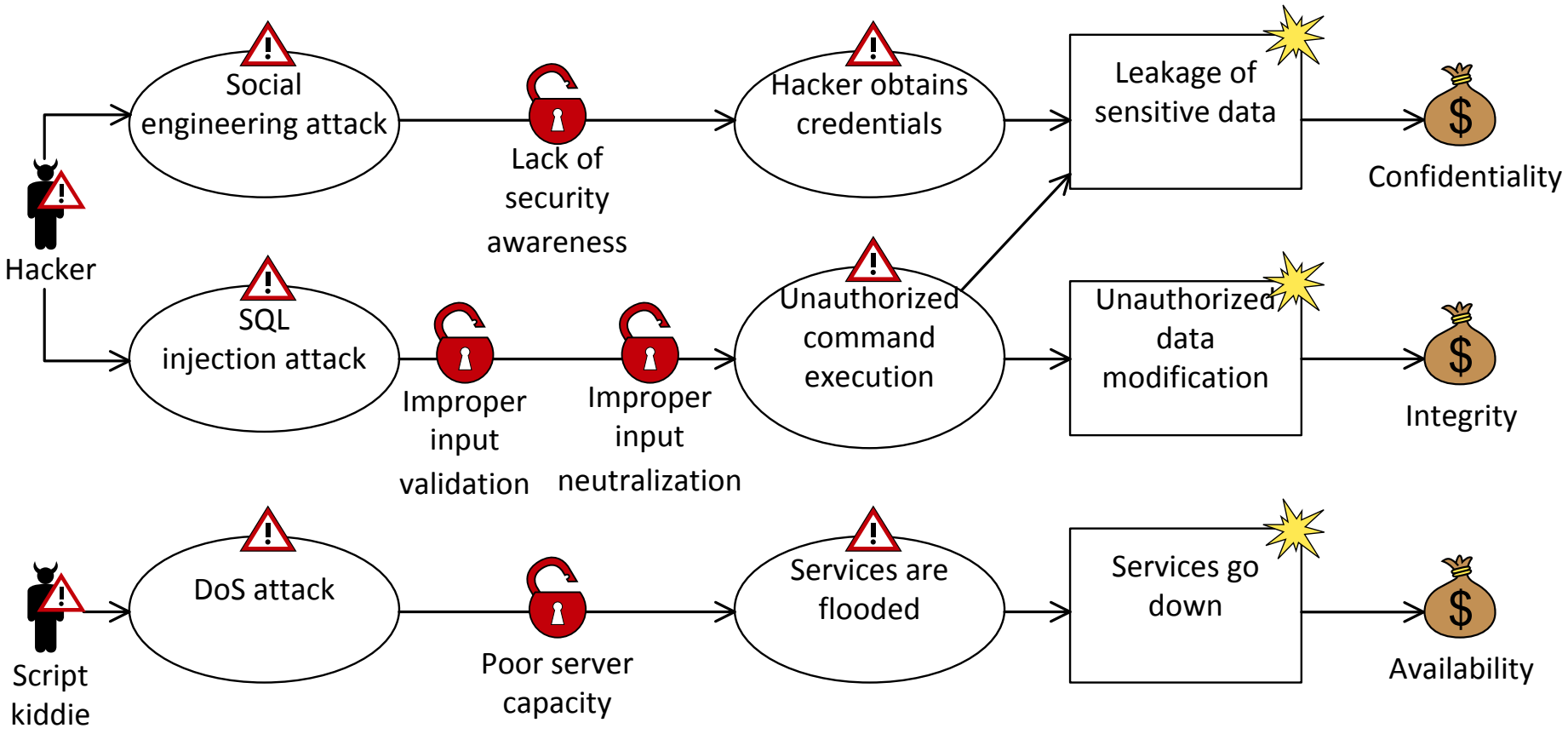
- Hva koster det?
- Hva er nytten?

- Først skal vi se nærmere på kost-nytte-analyse i risikoanalyse
- Deretter ser vi hvordan dette kan anvendes på cyber-forsikring

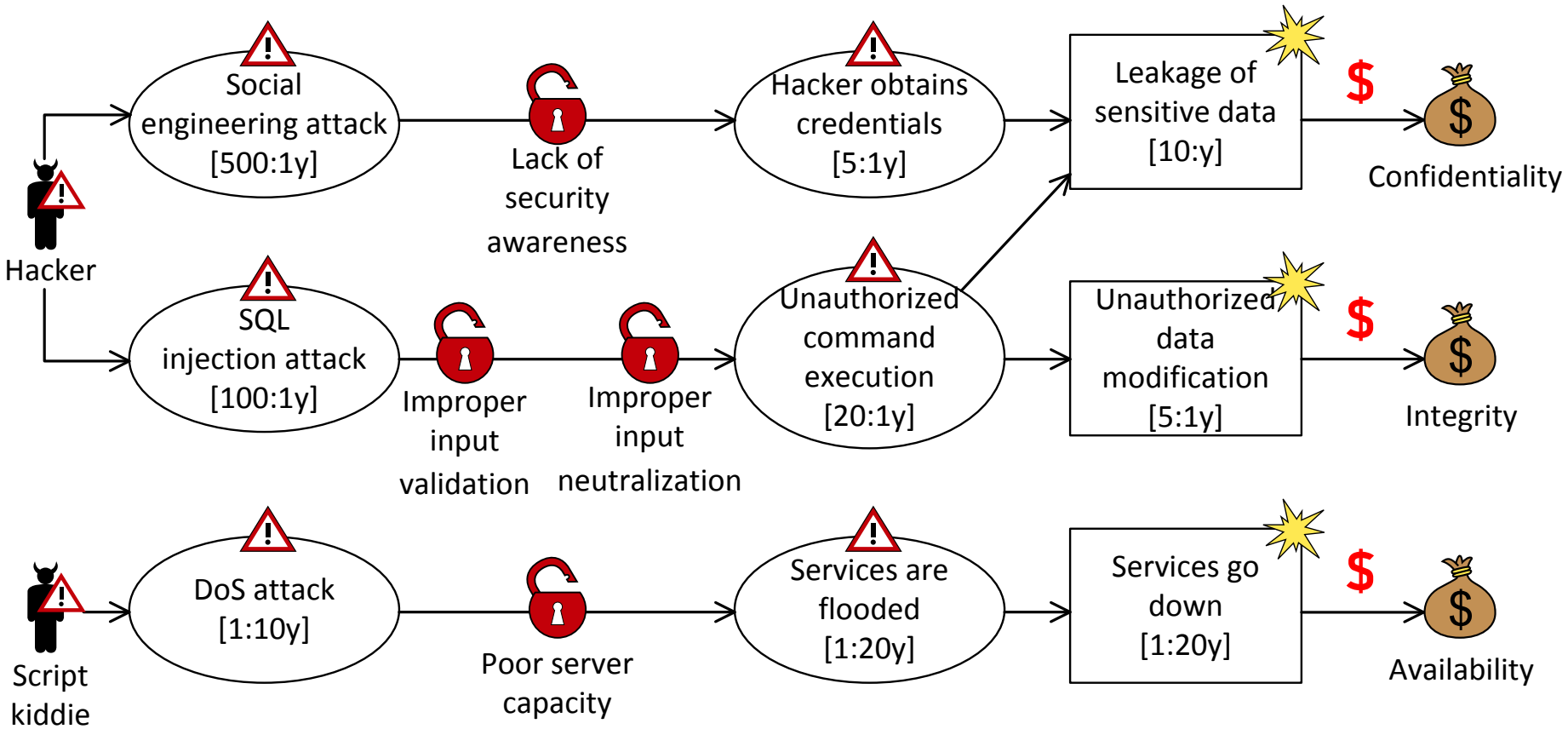
Noen begreper

- En **risiko** er sannsynligheten for en uønsket hendelse og dens konsekvens for et aktivum
- **Risikoverdien** beregnes ved å kombinere sannsynlighet og konsekvens
- En **behandling** er et tiltak for å redusere risiko

Eksempel: Cyber-risiko



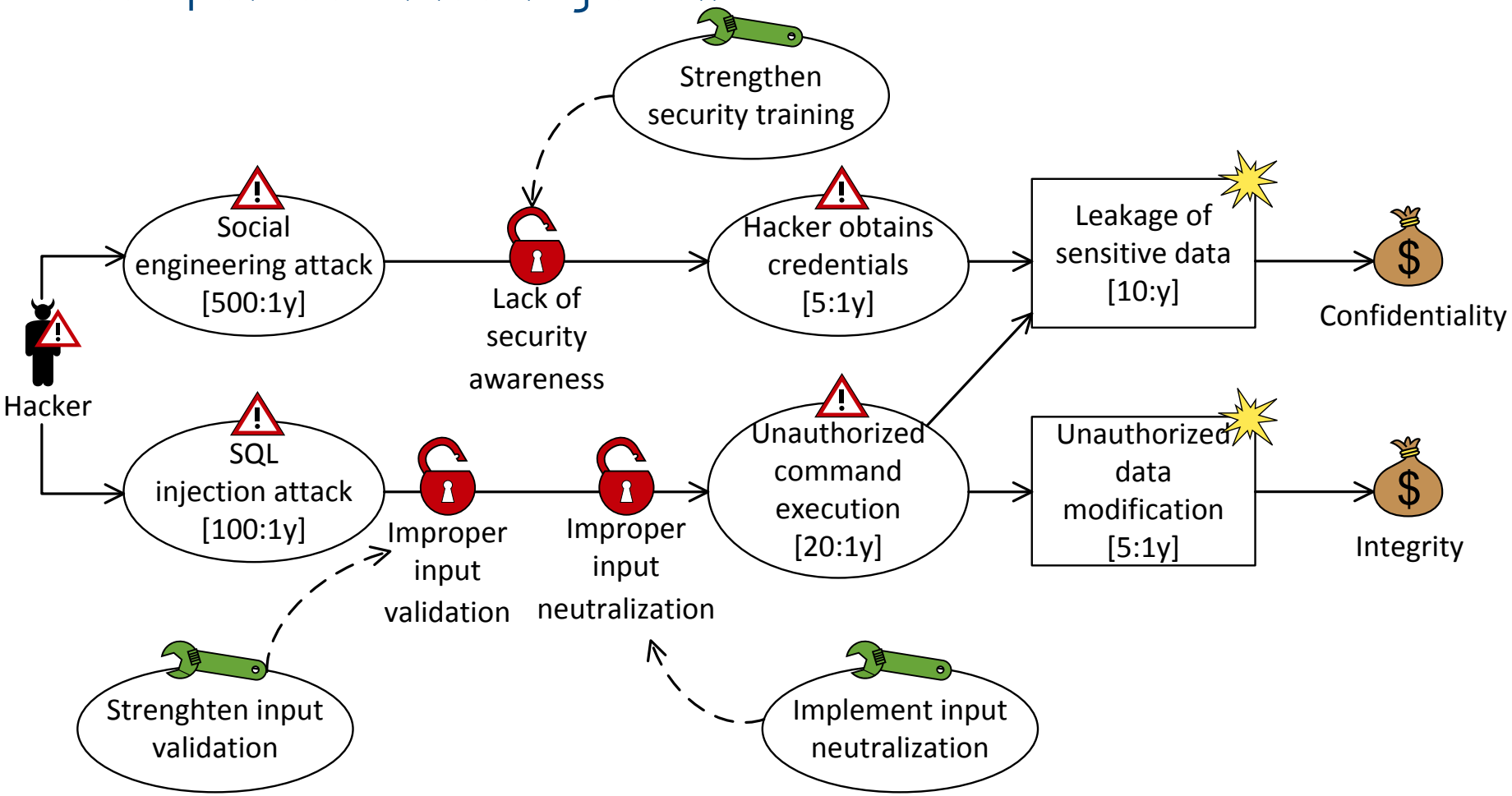
Eksempel: Risiko estimering



Elementer i estimering av kost

- Hvilke aktiva blir direkte skadet av hendelser?
- Hvilke aktiva blir indirekte skadet av hendelser?
- Hvilke immaterielle aktiva blir berørt?
- Hvilke sekundærtap følger av identifiserte primærtap?
  - F.eks. omdømmetap som en konsekvens av lekkasje
- Hva er reparasjonskostnadene?
- Finnes det rettslig ansvar og konsekvens?
- …

Eksempel: Identifisering av tiltak

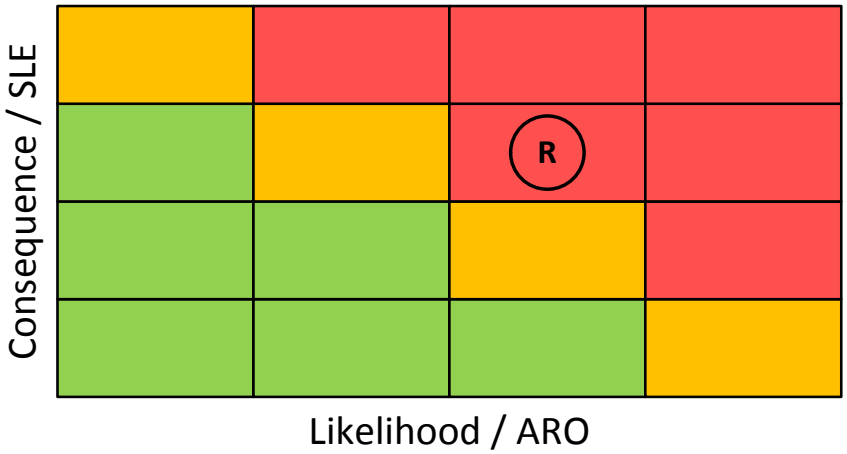


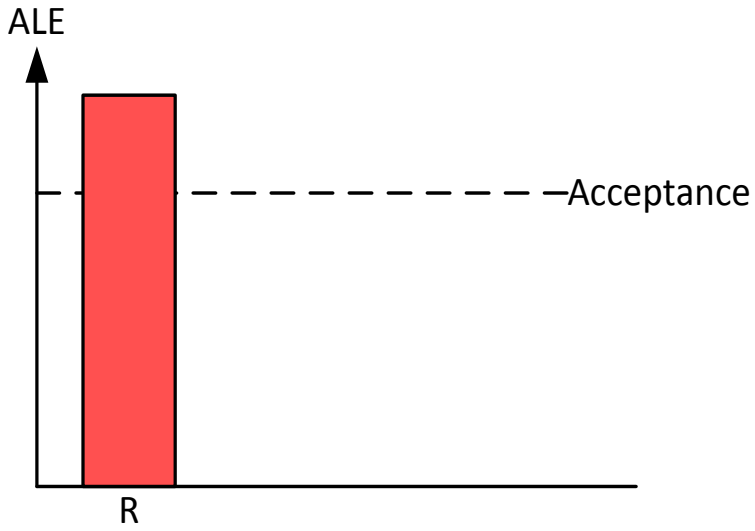
Analyse av tiltak

- Vi har utviklet støtte for modellering og analyse av tiltak
  - Kost av tiltak
  - Effekt av tiltak mht. sannsynlighet og konsekvens
  - Identifisering og sammenlikning av tiltaksalternativer
  - Presentasjon av kost-nytte-bildet for beslutningstakere
  - Normalisering av analyseresultater mht. *annualized loss expectency*

[Tran, Solhaug og Stølen, 2013]

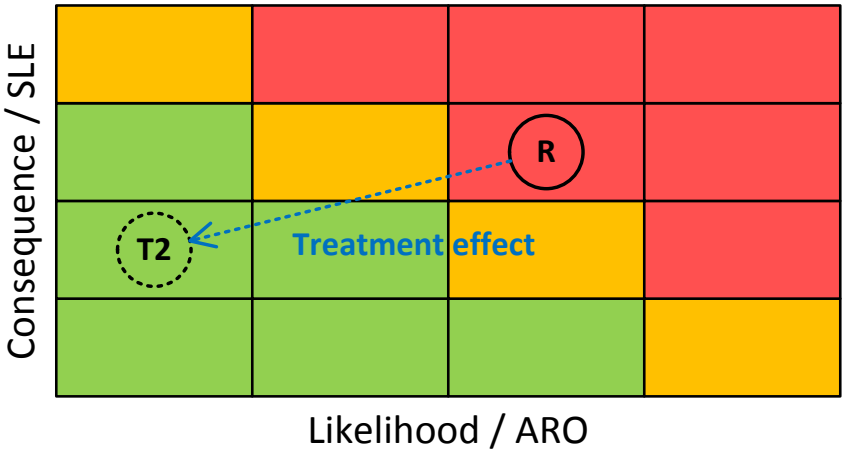
Risiko som forventet årlig tap



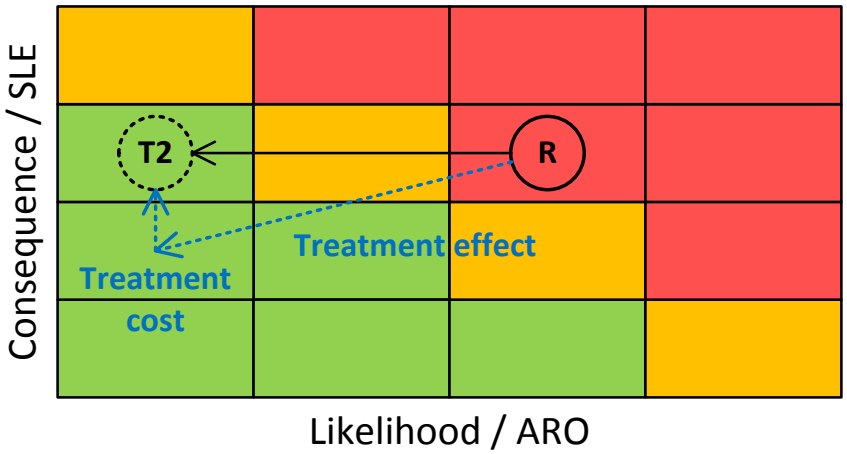


- SLE: Single loss expectency – Størrelsen på skaden til en uønsket hendelse
- ARO: Annual rate of occurrence – Årlig frekvens av uønsket hendelse
- ALE: Annualized loss expectency – Årlig tap gitt ved SLE x ARO

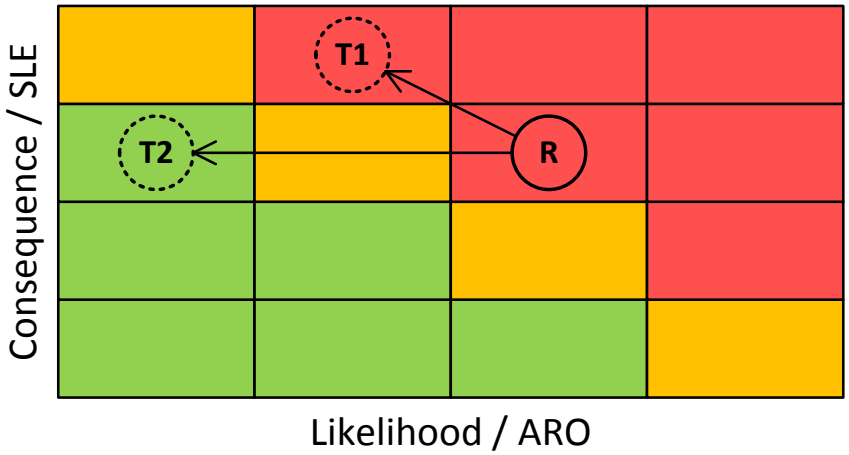
Kost-nytte-analyse av tiltak

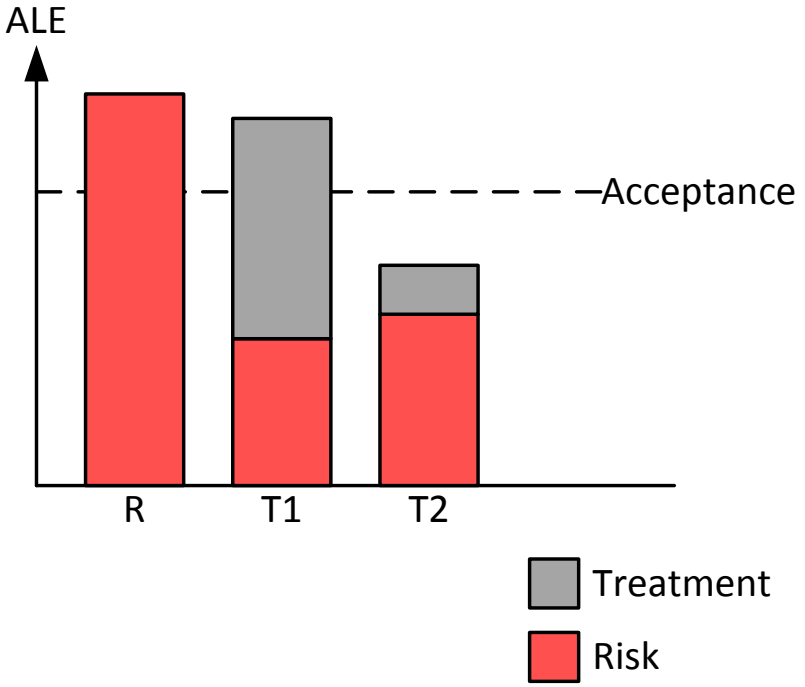


Kost-nytte-analyse av tiltak



Kost-nytte-analyse av tiltak





Cyber-forsikring

- Cyber-forsikring er overføring av finansiell risiko ved cyber-insidenter til en tredjepart
  - Se f.eks. [Böhme og Schwartz, 2010]

Cyber-forsikring – Eksempler

- Dekning av og kostnad for cyber-forsikring varier veldig mye mellom selskaper
- Elementer som ofte kan dekkes:
  - Juridisk ansvar og kostnad for sikkerhetsbrudd
  - Programmeringsfeil
  - Gjeninnsetning eller gjenoppbygging av data
  - Avbruddstap (business interruption losses)
  - Økte driftskostnader
  - PR-utgifter
  - Kundehåndtering
- "Cyber policies are still the Wild West of insurance policies"
  - Selena Linde (forsikringsjurist)
    www.darkreading.com/operations/10-things-it-probably-doesnt-know-about-cyber-insurance/d/d-id/1316862

Cyber-forsikring som behandling av risiko

- Krever forståelse av de økonomiske aspektene ved sikkerhet og risiko
  - Hva er kostnaden for å opprettholde nødvendig grad av sikkerhet?
  - Hvordan anslå verdien til informasjonsaktiva og andre immaterielle aktiva som omdømme?
  - Hva er den årlige økonomiske kostnaden ved å akseptere gitte risikoer?
  - Hva er kostnaden og nytteverdien av å behandle risikoer?
  - …
- Hva bør prisen være for å overføre risiko til en tredjepart?

Hva karakteriserer risikoer som kan forsikres?

- Stort antall eksponenter (grunnlag for prediksjon)
- Spesifikk hendelse (tid, sted, årsak)
- Tilfeldig hendelse (utenfor kontroll til forsikringstaker)
- Stor tap (skaden må være meningsfull å forsikre seg mot)
- Rimelig (*affordable*) premie
- Kan estimeres (sannsynlighet for og størrelse av tap)
- Begrenset risiko for katastrofalt store tap (spredning av forsikrer sin risiko)

[Mehr og Cammack, 1980]

Kan cyber-risiko forsikres?

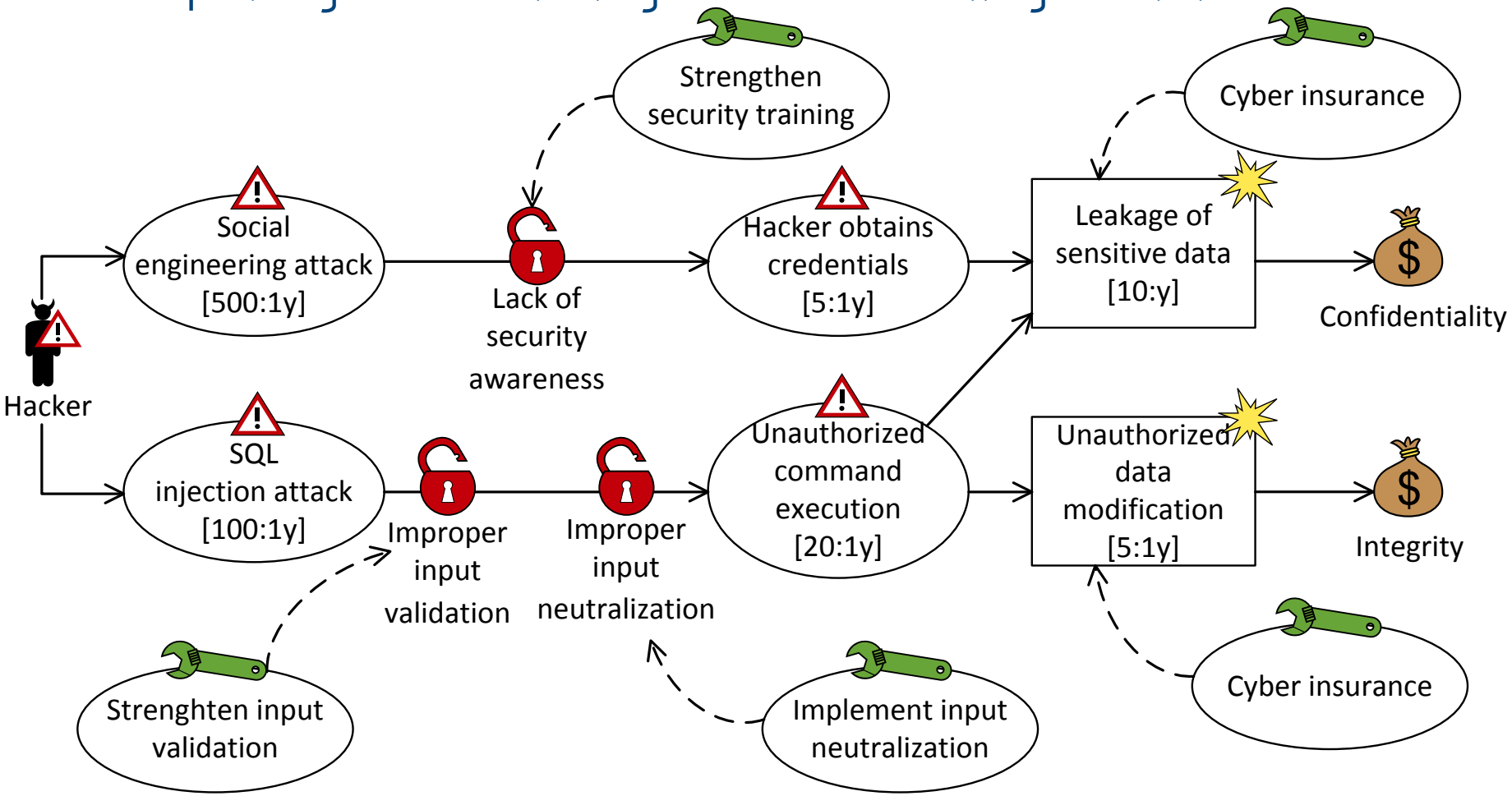
- Det er i alle fall et marked for det, spesielt i USA
  - Raskest voksende nisjeforsikringen i USA
  - På vei inn i Europa og Norge
- Men markedet og produktet er umodent
  - Se, for eksempel [Toregas og Zahn, 2014] og [ENISA, 2012]

- Blant annet er det behov for kost-nytte-analyse i relasjon til cyber-sikkerhet og cyber-risiko

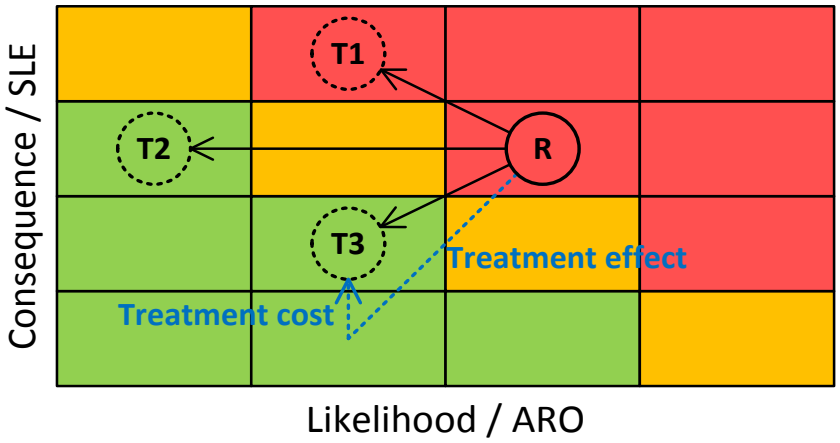
Når bør bedrifter ha cyber-forsikring?

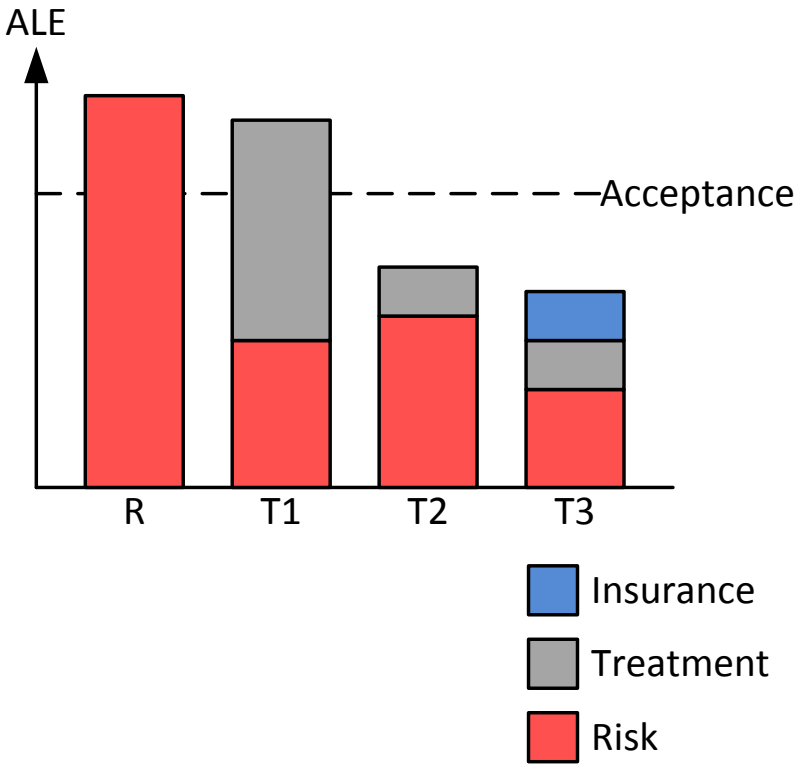
- Elementer som er relevante:
  - Når det er billigere enn å sørge for sikkerheten selv
  - Når usikkerheten er stor
  - Når konsekvensen potensielt er katastrofal
  - Når man ikke har kapasitet til selv å håndtere konsekvensene av store hendelser

Eksempel: Cyber-forsikring som behandling av risiko



Kost-nytte-analyse av tiltak og cyber-forsikring

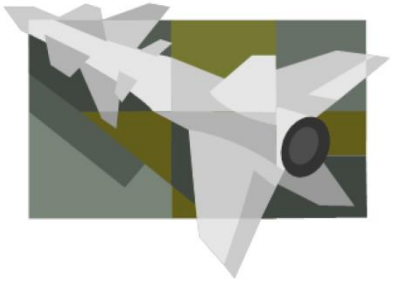




Men hva med angripers kost og nytte?

- Kost-nytte-analyse kan også bidra til vurdering av trusler

a) Cost of preventive action (a)
b) Cost of remedial action (b>a)
c) Loss (c>>a+b)
d) Cost of insurance (d>a+b)
e) Insurance payout (e<c)



f) Cost of attack (f)
g) Profit (g>>f)
h) Penalty (h<<g)

Oppsummering

- Cyberrisiko innebærer ofte finansiell risiko for bedrifter
- Cyberforsikring er å overføre denne finansielle risikoen til en tredjepart
- Produktet og markedet er imidlertid umodent
- Blant annet er det behov for teknikker for å analysere og evaluere kost og nytte mht. cybersikkerhet, cyberrisiko, risikobehandling og cyberforsikring
- En av utfordringene i den forbindelse er hvordan å forstå sikkerhet, risiko og aktiva i termer av kroner og øre

Referanser

- R. Böhme and G. Schwartz. Modeling cyber-insurance: Towards a unifying framework. Workshop on the Economics of Information Security (WEIS). Harvard, 2010
- European Network and Information Security Agency . Incentives and barriers of the cyber insurance market in Europe. ENISA, 2012
- R. Mehr and E. Cammack. Principles of Insurance, 7th ed. RD Irwin, 1980
- C. Toregas and N. Zahn. Insurance for cyber attacks: The issue of setting premiums in context. Report GW-CSPRI-2014-1, The George Washington University, 2014
- L. M. S. Tran, B. Solhaug and K. Stølen. An approach to select cost-effective risk countermeasures. In Proc. 27th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy (DBSec'13). LNCS 7964, pp. 266-273, Springer, 2013.
- World Economic Forum. Global Risks 2015. Insight report, 2015

Relaterte prosjekter

InSecurance

www.sintef.no/insecurance

RASEN

www.rasenproject.eu