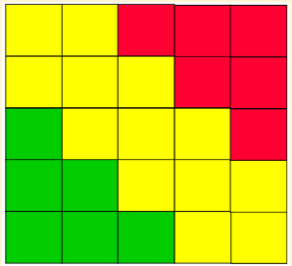
VI BEHÖVER MER KVANTITATIV RISKANALYS!

December 2020

Martin Bergling

Kvalitativa metoder…



cybernode.se

RI.
SE

Den svenska noden för att accelerera innovation och forskning inom cybersäkerhet

Martin Bergling, koordinator
martin.bergling@ri.se
070-982 4730

RISE Cybersecurity, Stockholm/Kista
Shahid Raza, enhetschef

SVERIGES FÖRSTA TELEGRAFSTOLPE

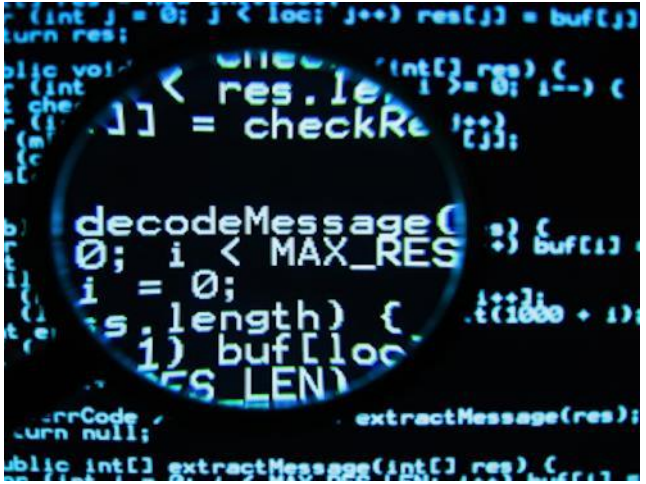
- 15 maj 1853
- Stockholm-Uppsala

DAGSLÄGET…

- Transportstyrelsen
- GDPR
- NIS-direktivet
- Ny säkerhets-skyddslag
- 1177
- EU Cyber Security Act

ÄR IT-SÄKERHETSOMRÅDET SPECIELLT?

- **Ja!**
- Programvara lyder inte under naturlagar
  - ex. skalning, automatisering
- ”Logisk jordbävning”
  - var som helst, när som helst
- IT-branschen fortfarande oerfaren
- Angripare
  - globala
  - anonyma



AI
Big Data

Få stora IT-aktörer
Aggressiva statsaktörer

DEN GLOBALA ATTACKYTAN ÖKAR

- Fler sårbarheter
- Fler kunniga angripare
- Fler personer på Internet
- Ökat nätberoende
  - enskilda
  - organisationer
- ==> Risk för kaskadeffekt

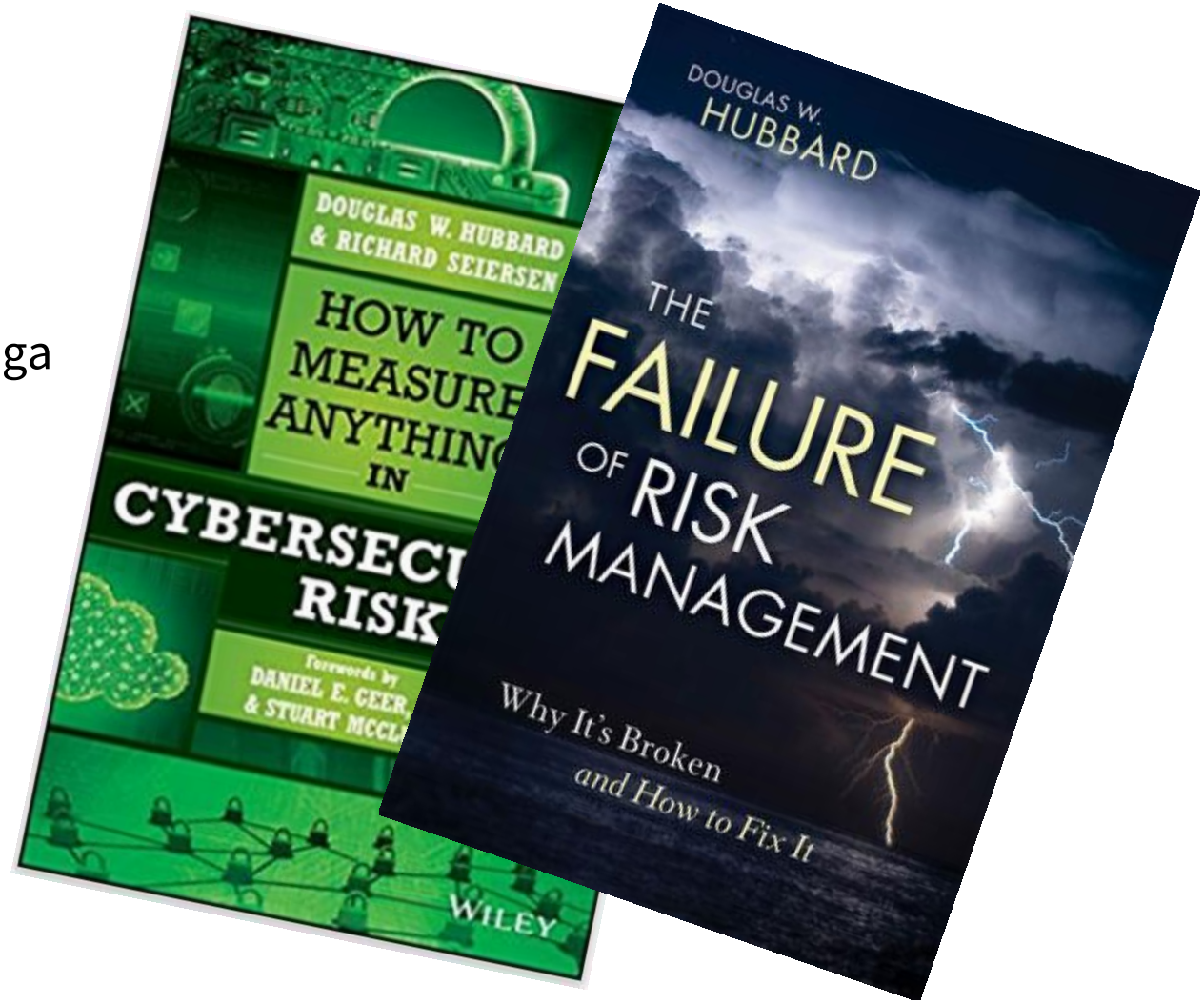
AGENDA

- Riskanalys
  - Boken
  - Problem idag
  - En bättre metod
    - Monte Carlo!
    - Demo
  - Hur införa i organisationen?
  - Frågor och diskussion

BOKEN

- Väl underbyggd
- Många vetenskapliga referenser

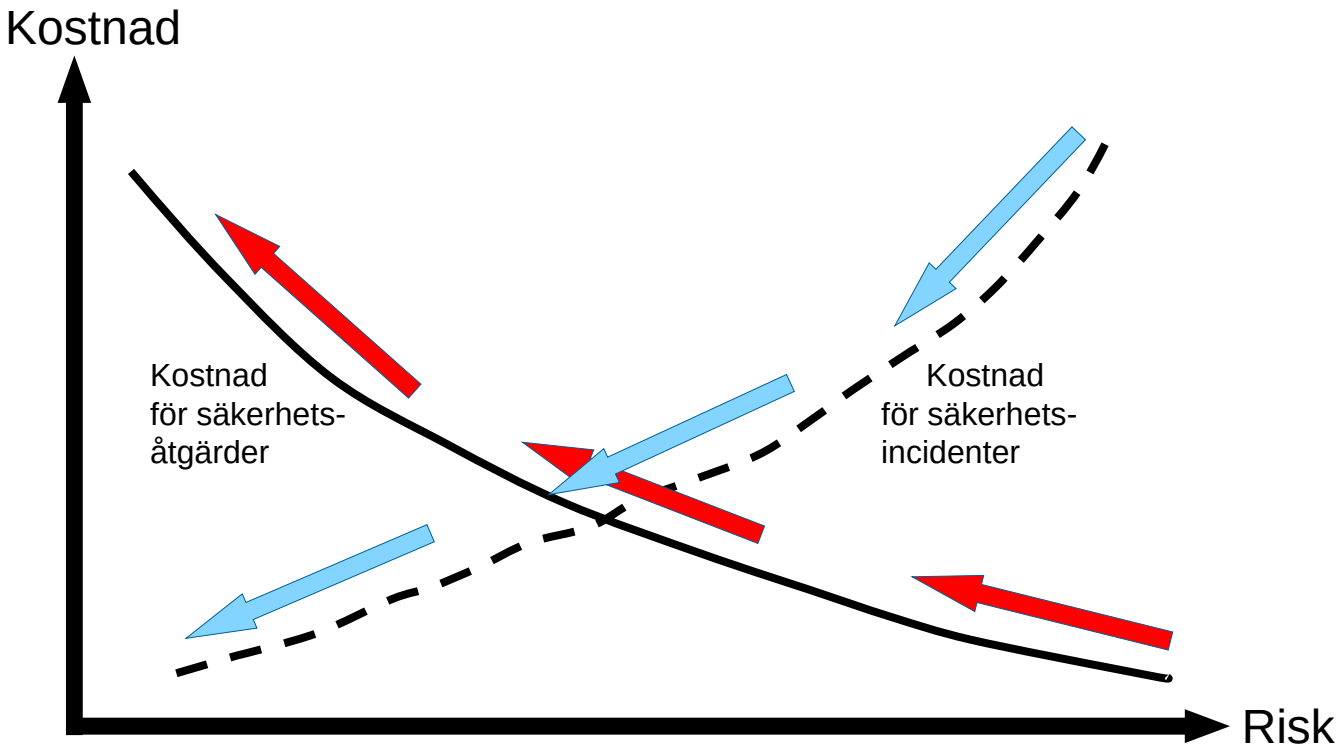
SIG Security
Fem bokcirklar
2017-2021



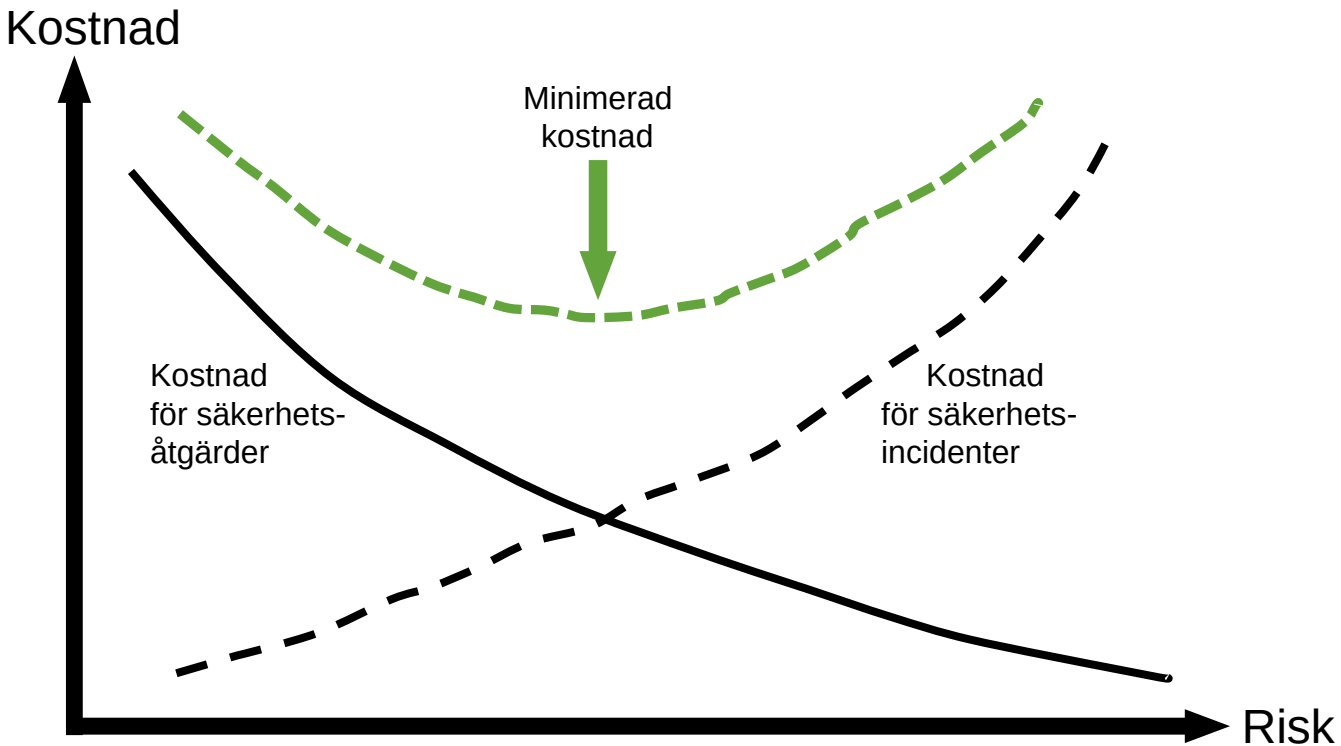
BOKENS HUVUDBUDSKAP

- Analysen ska ge beslutsunderlag
- Dagens enkla (kvalitativa) matrismetod
  - Fungerar inte bra!
  - Bättre riskanalys den viktigaste ’patchen’!
- Kvantitativ metodik
  - Välbeprövat, fungerar bra
  - Mätdata finns!
- Experter
  - Inte så bra som vi tror!

KOSTNAD KONTRA RISK

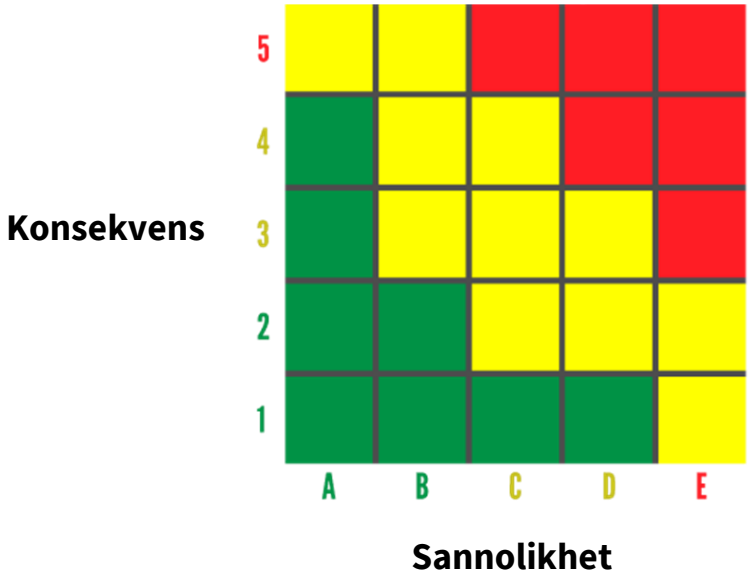


KOSTNAD KONTRA RISK



”MATRISMETODEN” (1)

- Arbetssätt
  - Ta fram en risklista
  - Prioritera
  - Bedöm sannolikhet
  - Bedöm konsekvens
  - Sammanställ riskmatris
  - Prioritera
  - Utforma åtgärdsplan



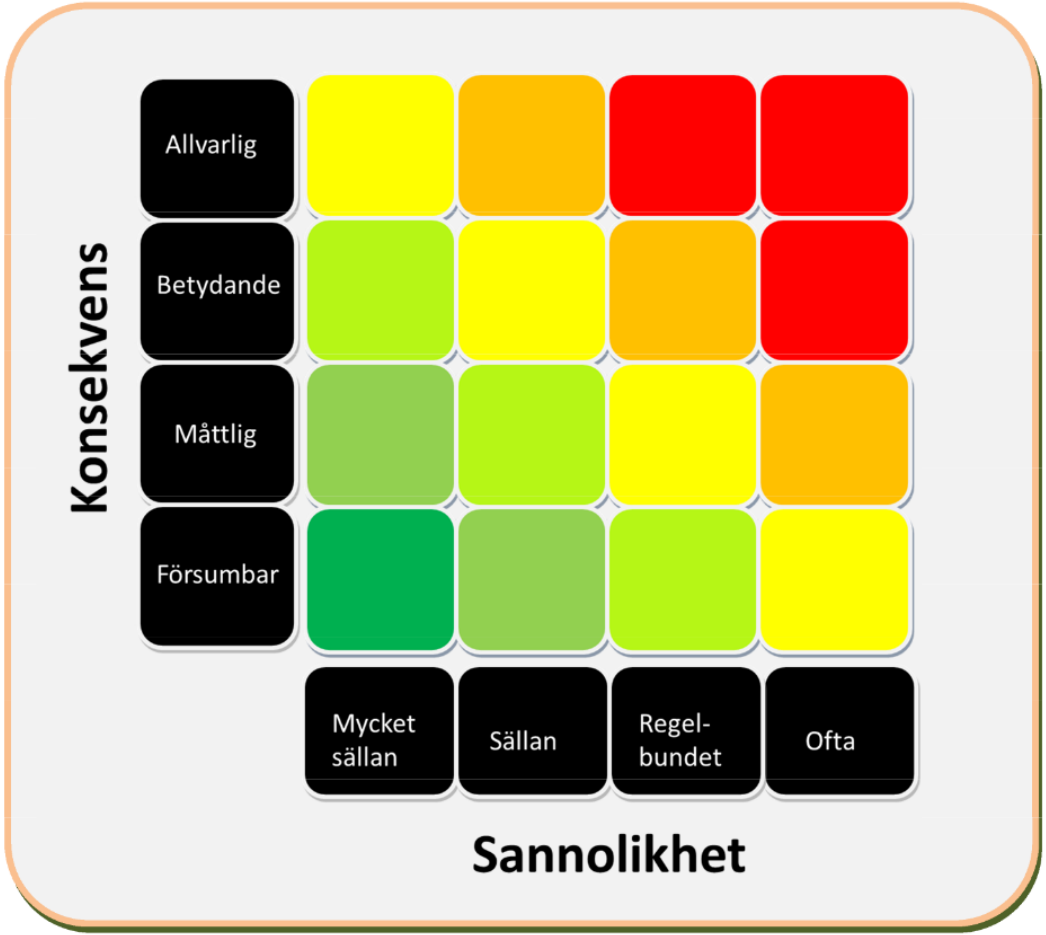
”MATRISMETODEN” (2)

- Enkelhet
  - lätt att förstå
  - lätt att använda
- Tydlighet
  - skapar engagemang
  - underlättar kommunikation
    - ledning
    - medarbetare

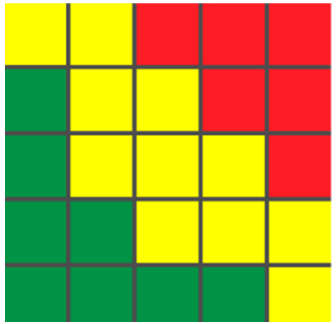
Skenbar tydlighet!

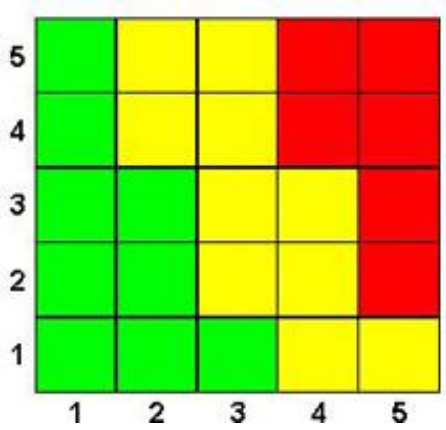
”MATRISMETODEN” (3)

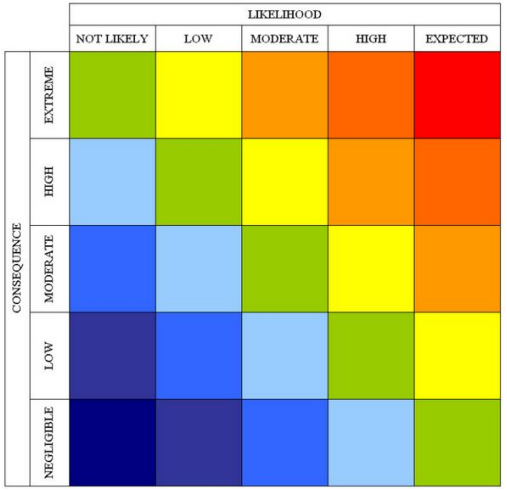
- Vaga skalor
  - även om förtydliganden ofta sker



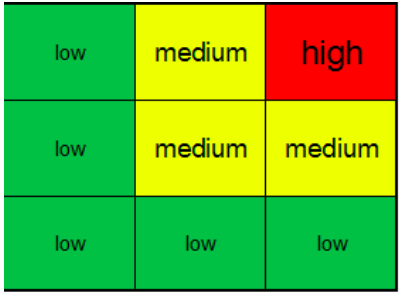
EXEMPEL




5
4
3
2
1
1 2 3 4 5

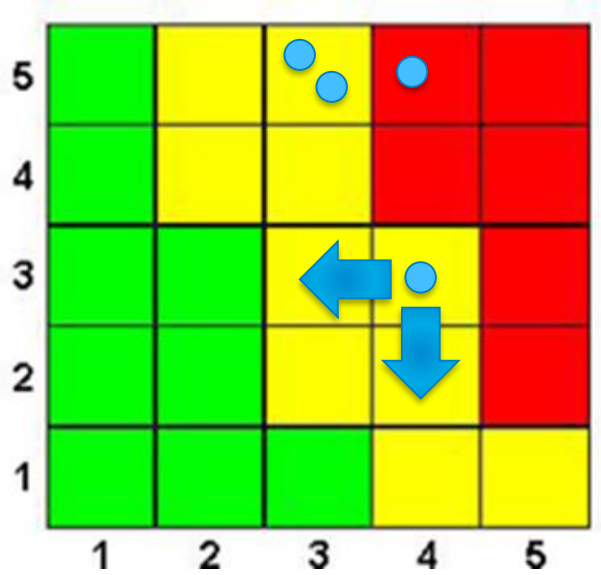

LIKELIHOOD
NOT LIKELY
LOW
MODERATE
HIGH
EXPECTED
CONSEQUENCE
EXTREME
HIGH
MODERATE
LOW
NEGLIGIBLE


5 5 10 15 20 25
4 4 8 12 16 20
3 3 6 9 12 15
2 2 4 6 8 10
1 1 2 3 4 5
1 2 3 4 5


low medium high
low medium medium
low low low

EXEMPEL PÅ PROBLEM

- Är det bättre att hantera två gula än en röd risk?
- Är det effektivast att minska sannolikheten eller konsekvensen för en risk?



FLER FRÅGOR ATT BESVARA…

- Vilka risker är mest intressanta att kartlägga bättre?
  - Enkelt att komplettera analysen med ny kunskap?
- Hur mycket minskar risken med en viss åtgärd?
- Efter årets investeringar, hur mycket har den totala risken minskat?
  - Hur stor säkerhetsbudget bör vi föreslå?

EXPERTER…

- *”Jo, men vi har ju säkerhetsexperter som gör välavvägda bedömningar utifrån lång erfarenhet… ”*

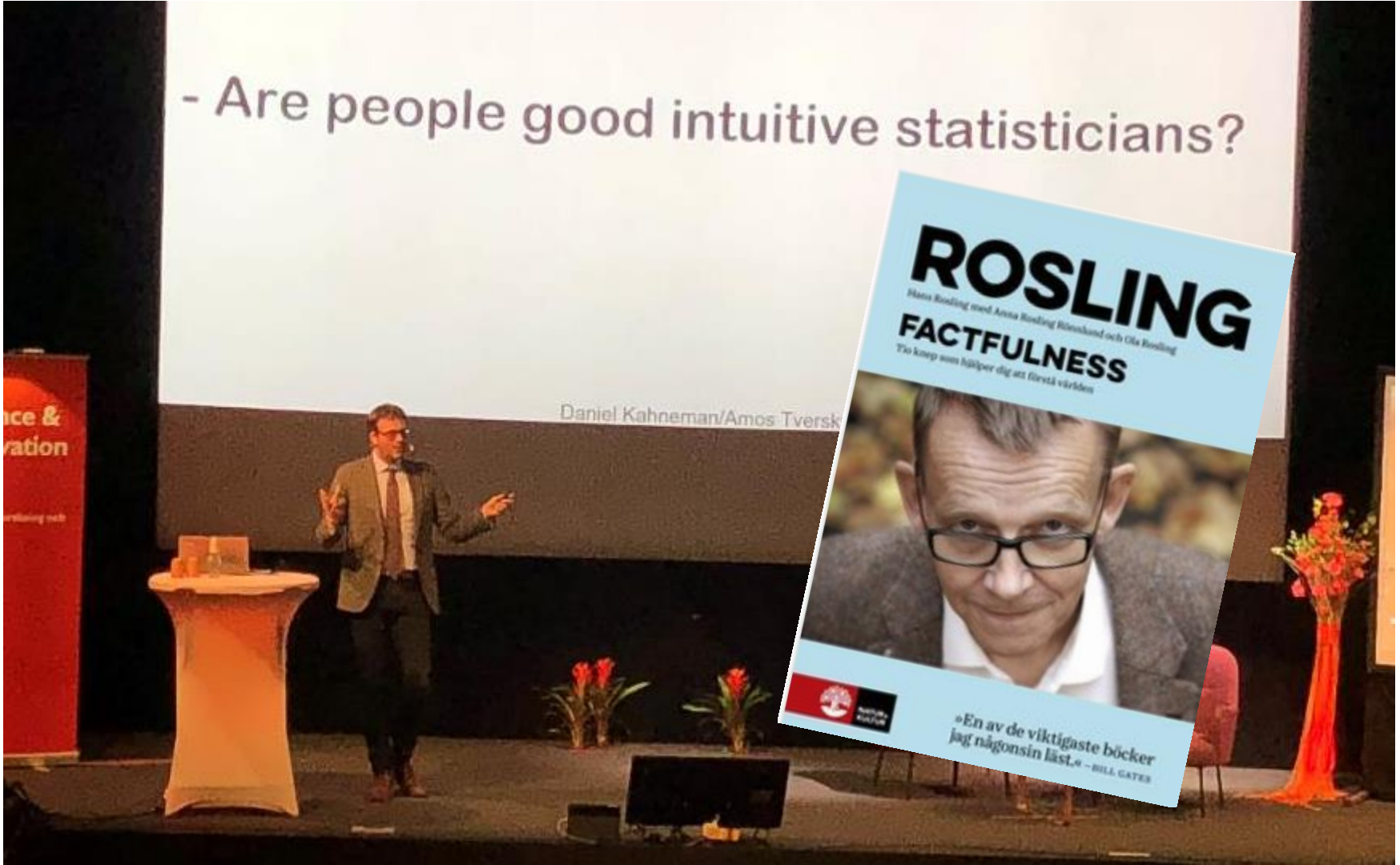
DET ÄR SVÅRT ATT SIA, SPECIELLT OM FRAMTIDEN…

- Svårt även för experter
- Lärande kräver återkoppling
  - omedelbar
  - regelbunden
  - otvetydig
- Vi minns selektivt
  - näraliggande
  - positiva

  ➔ bedömningar baseras på selektiva minnen

EXPERIMENT AV PHILIP TETLOCK

- Frågade 284 experter
  - politik och ekonomi
  - frågor om vad som kan förväntas hända i en nära framtid
  - oftast tre svarsalternativ
- 82.000 förutsägelser…
- Resultat:
  - Mindre än en tredjedel var rätt!
  - Sämre än slumpen!


- Are people good intuitive statisticians?
Daniel Kahneman/Amos Tversk
ROSLING
Hans Rosling med Anna Rosling Rönnlund och Ola Rosling
FACTFULNESS
Tio knep som hjälper dig att förstå världen
»En av de viktigaste böcker jag någonsin läst.« – BILL GATES

ATT FÖRUTSE FRAMTIDEN

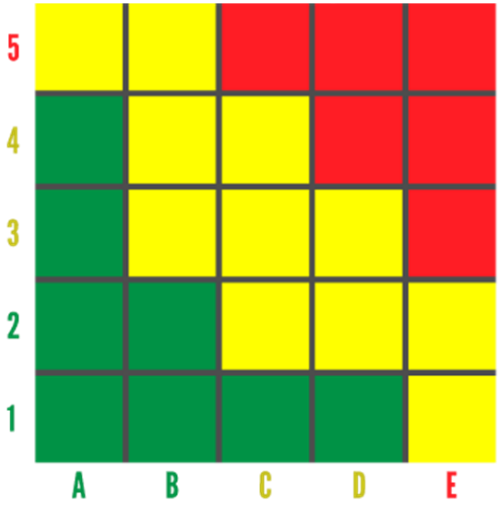
- Enkla statistiska metoder är oftast bättre!
  - historiska data
  - korrekt matematik
- Experter kan ”kalibreras”
  - bättre bedöma sin egen osäkerhet
  - därmed ange sannolikheter mer korrekt

AGENDA

- Riskanalys
  - Boken
  - Problem idag
  - En bättre metod
    - Monte Carlo!
    - Demo
  - Hur införa i organisationen?
  - Frågor och diskussion

EN BÄTTRE RISKANALYS (1)

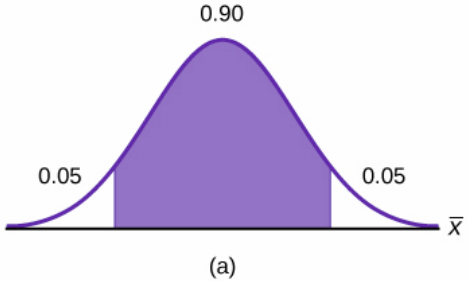
- Arbetssätt
  - Ta fram en risklista
  - Prioritera
  - Bedöm sannolikhet
  - Bedöm konsekvens
  - Sammanställ riskmatris
  - Prioritera
  - Utforma åtgärdsplan



EN BÄTTRE RISKANALYS (2)

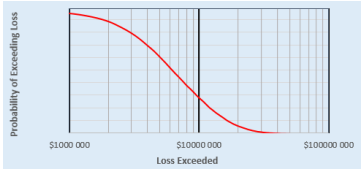
- Arbetssätt
  - Ta fram en risklista
  - Prioritera
  - ~~Bedöm sannolikhet~~
  - ~~Bedöm konsekvens~~
  - ~~Sammanställ riskmatris~~
  - Prioritera
  - Utforma åtgärdsplan

- Bestäm tidsperiod
- Bedöm sannolikhet
  - 0%-100%



- Bedöm ”förlustintervall” som ett 90% konfidensintervall

- Excel: simulera 10.000 gånger
- Beräkna ”nulägeskurvan”



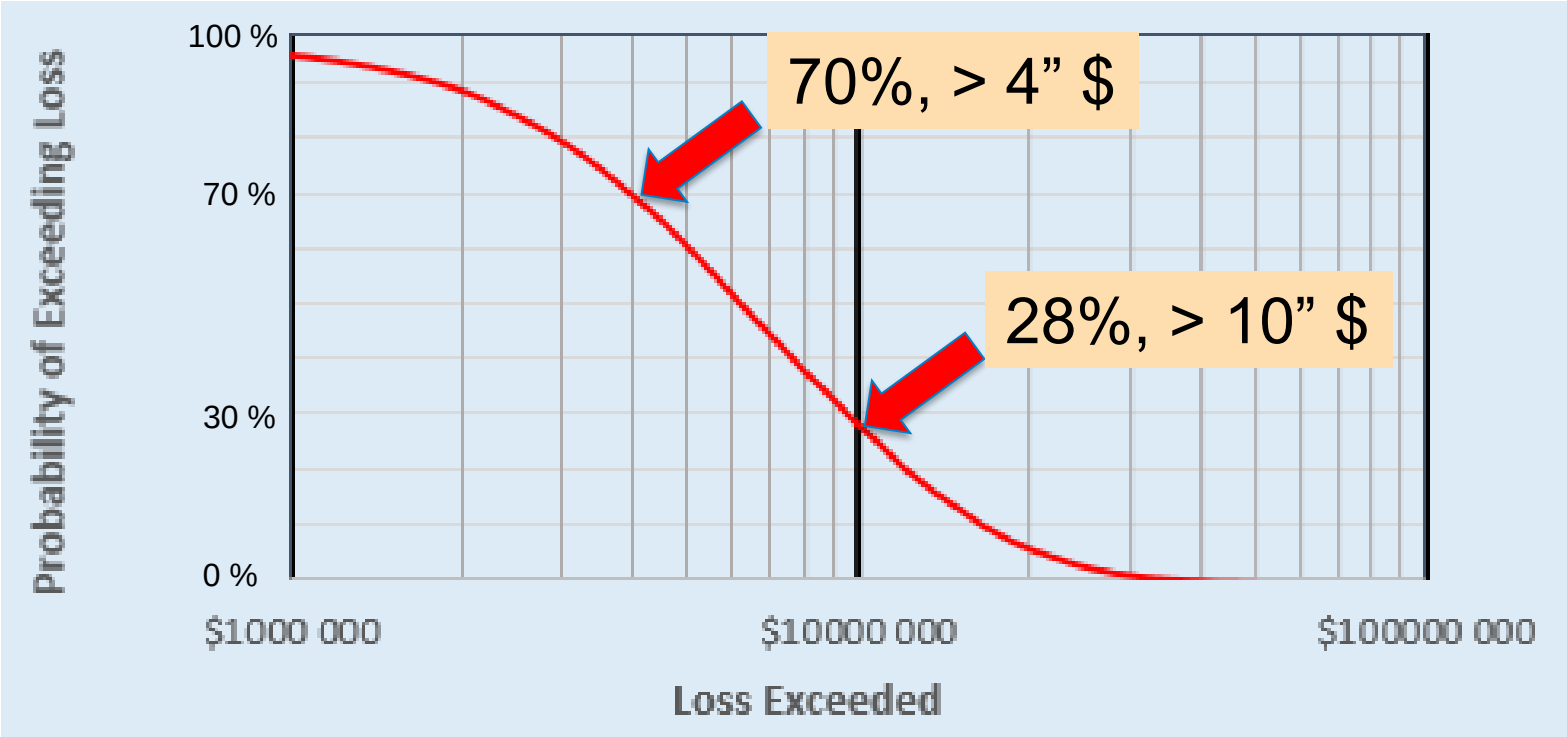
EXCEL-ARKET

Event Name	Prob. Event Will Happen (Annual)	90% Confidence Interval of Impact		Expected Loss
		Lower Bound	Upper Bound	
Event 1	11,0%	$ 2 000 000	$ 20 000 000	$ 888 802
Event 2	5,0%	$ 500 000	$ 2 000 000	$ 54 643
Event 3	10,0%	$ 400 000	$ 2 500 000	$ 116 785
Event 4	40,0%		5 000 000	$ 573 612
Event 5			500 000	$ 33 850
Event 6		$ 200 000	$ 5 000 000	$ 193 677
Event 7	10,0%	$ 20 000	$ 750 000	$ 22 471

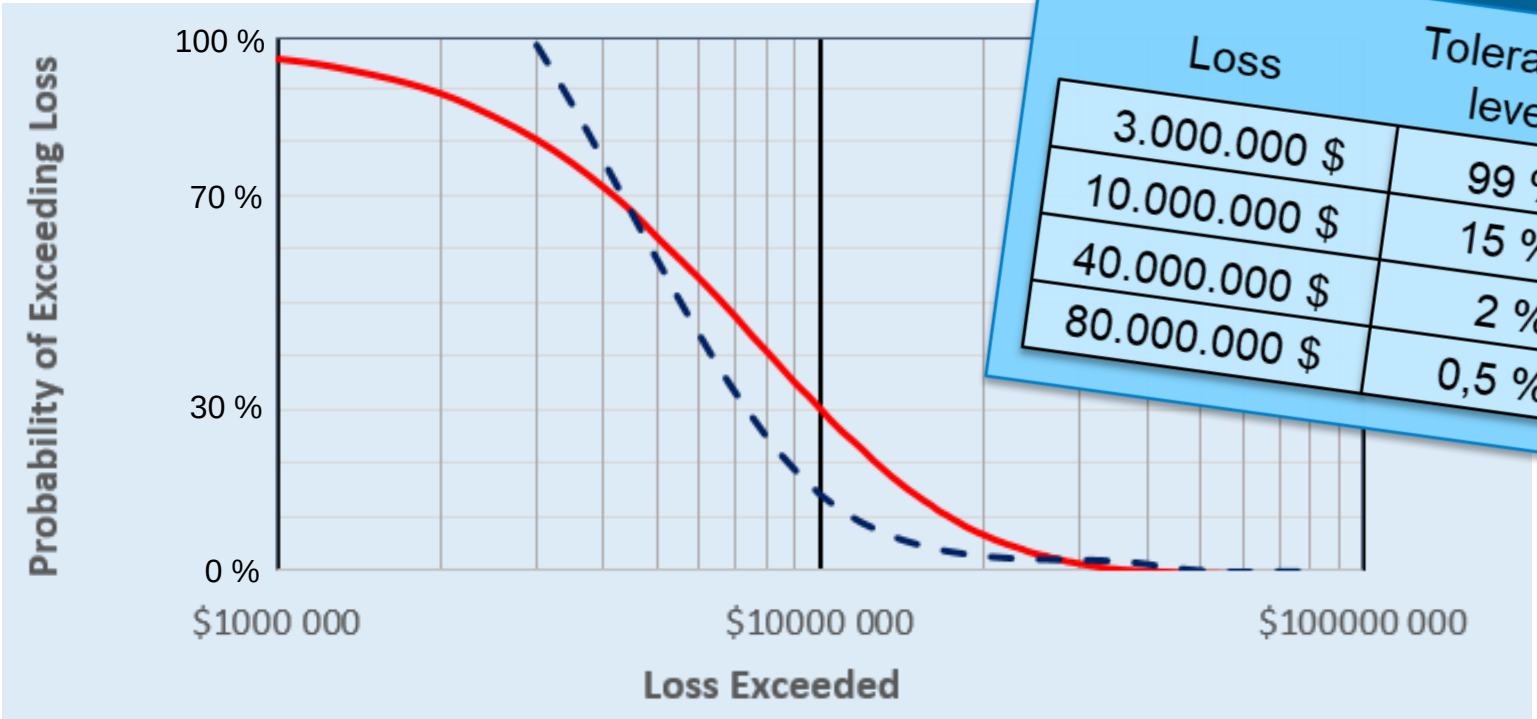
Simulering!

EN ”MINSTA FÖRLUST-KURVA”

Loss Exceedance Curve



RISKTOLERANSKURVAN



Risk Tolerance

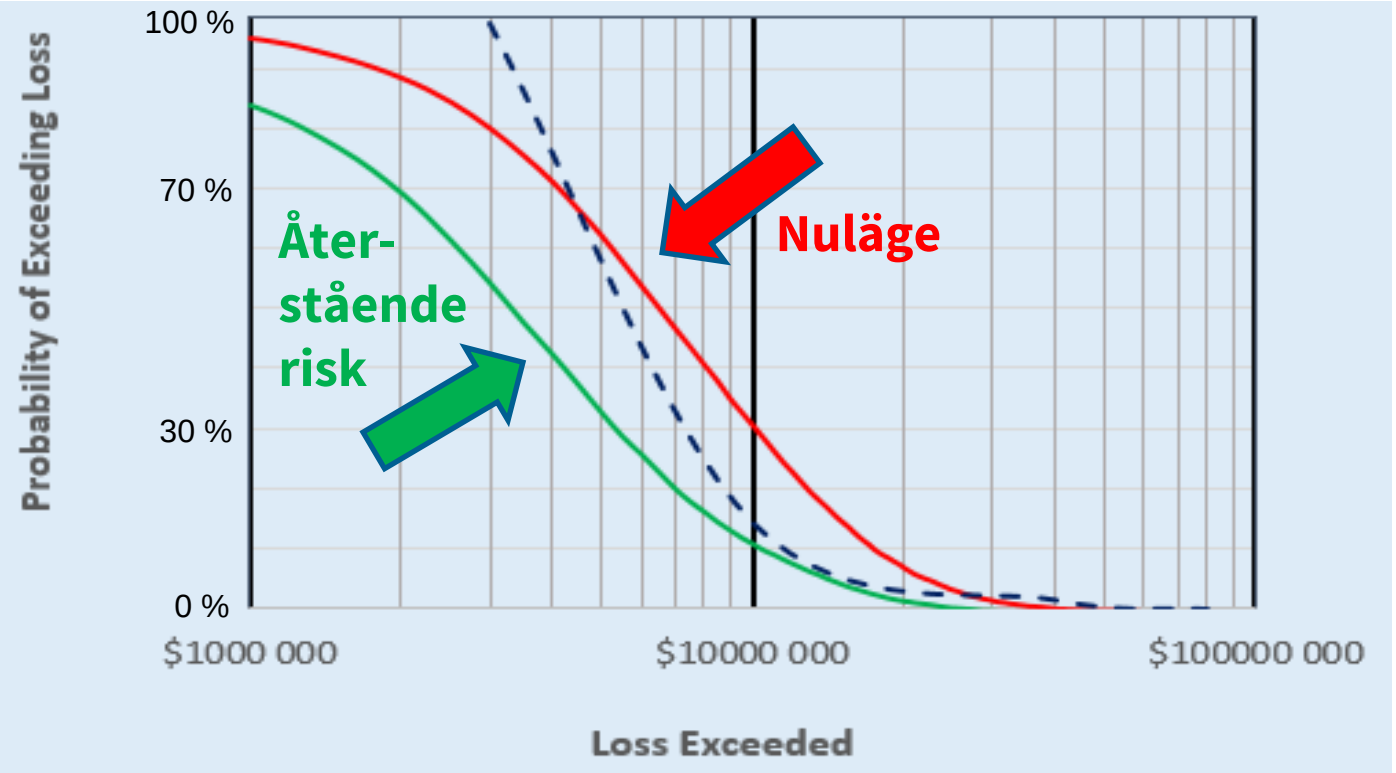
Loss	Tolerance level
3.000.000 $	99 %
10.000.000 $	15 %
40.000.000 $	2 %
80.000.000 $	0,5 %

ANGE ÅTGÄRDSKOSTNAD + EFFEKTIVITET

Event Name	Prob. Event Will Happen (Annual)	90% Confidence Interval of Impact		Expected Loss	Cost of Proposed Mitigation	Reduction in Likelihood of Event From Mitigation	Return on Control
		Lower Bound	Upper Bound				
Event 1	11,0%	$ 2 000 000	$ 20 000 000	$ 888 802	$ 100 000	50%	344%
Event 2	5,0%	$ 500 000	$ 2 000 000	$ 54 643			0%
Event 3	10,0%	$ 400 000	$ 2 500 000		100 000	50%	-42%
Event 4	40,0%	$ 100 000			50 000	25%	187%
Event 5	20,0%	$					0%
Event 6	12,0%	$		193 677	$ 40 000	90%	336%
Event 7	10,0%	$	$ 750 000	$ 22 471			0%

Ny simulering!

RESIDUAL-KURVAN



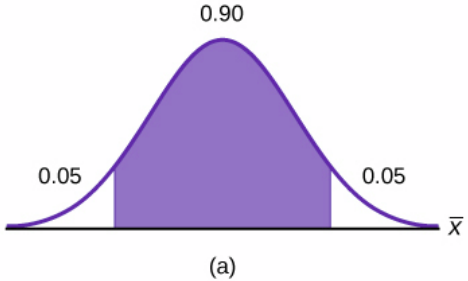
DEMONSTRATION AV EXCEL-ARKET…

www.howtomeasureanything.com/cybersecurity

EN BÄTTRE RISKANALYS (3)

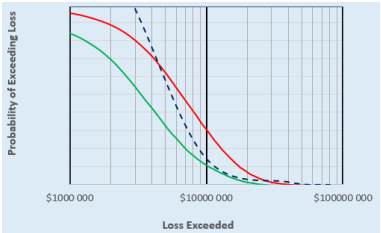
- Arbetssätt
  - Ta fram en risklista
  - Prioritera
  - ~~Bedöm sannolikhet~~
  - ~~Bedöm konsekvens~~
  - ~~Sammanställ riskmatris~~
  - Prioritera
  - Utforma åtgärdsplan

- Bestäm tidsperiod
- Bedöm sannolikhet
  - 0%-100%



- Bedöm ”förlustintervall” som ett 90% konfidensintervall

- Excel: simulera 10.000 gånger
- Beräkna ”nulägeskurvan”



- Undersök riskerna, välj åtgärder, jämför med risktoleranskurvan

FLER FRÅGOR ATT BESVARA…

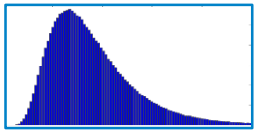
- Vilka risker är mest intressanta att kartlägga bättre?
  - Enkelt att komplettera analysen med ny kunskap?
- Hur mycket minskar risken med en viss åtgärd?
- Efter årets investeringar, hur mycket har den totala risken minskat?
  - Hur stor säkerhetsbudget bör vi föreslå?

SAMMANFATTNING AV METODEN

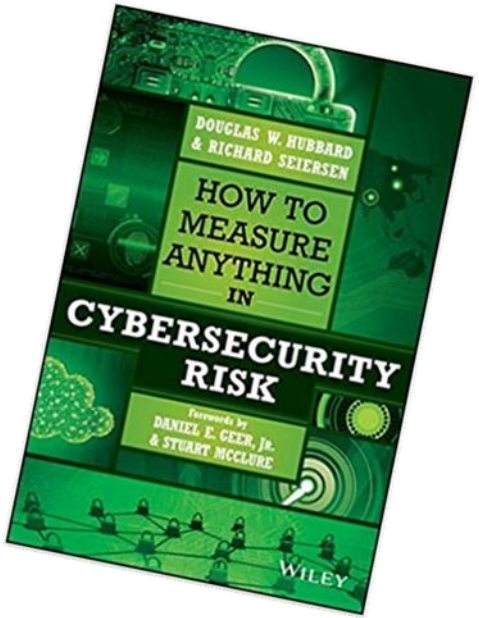
- Genom att
  - uppskatta ”förlustintervall” istället för konsekvenser
  - göra Monte Carlo-simuleringar i Excel
- så kan vi
  - få en bild av den samlade risken
  - studera enskilda riskers påverkan på den samlade risken
  - göra bättre bedömningar av var investeringar bör göras
  - uppdatera analysen med ny kunskap
  - kommunicera tydligare med ledningen

NÅGRA ORD TILL OM VAD BOKEN INNEHÅLLER

- Vad mätning innebär
  - ’*Uncertainty*’
- ”Kalibrering” av experter
- Statistiska metoder
  - Olika fördelningar



- Uppdelning i riskkomponenter
- Hur införa ny metodik i en organisation



FUNDERINGAR… (1)

- Svårbedömda konsekvenser
  - lagbrott
  - liv och hälsa
  - anseende

FUNDERINGAR… (2)

- Oberoende risker
  - …men beroenden finns
  - Inte en showstopper
  - Motfråga: hur hanteras det i ”matrisen”??
- Åtgärder som motverkar flera risker?
  - Kan delas upp i Excel
- Identifiering av risker
  - Har vi hela riskbilden?

AGENDA

- Riskanalys
  - Boken
  - Problem idag
  - En bättre metod
    - Monte Carlo!
    - Demo
  - Hur införa i organisationen?
  - Frågor och diskussion

STRATEGI FÖR INFÖRANDE

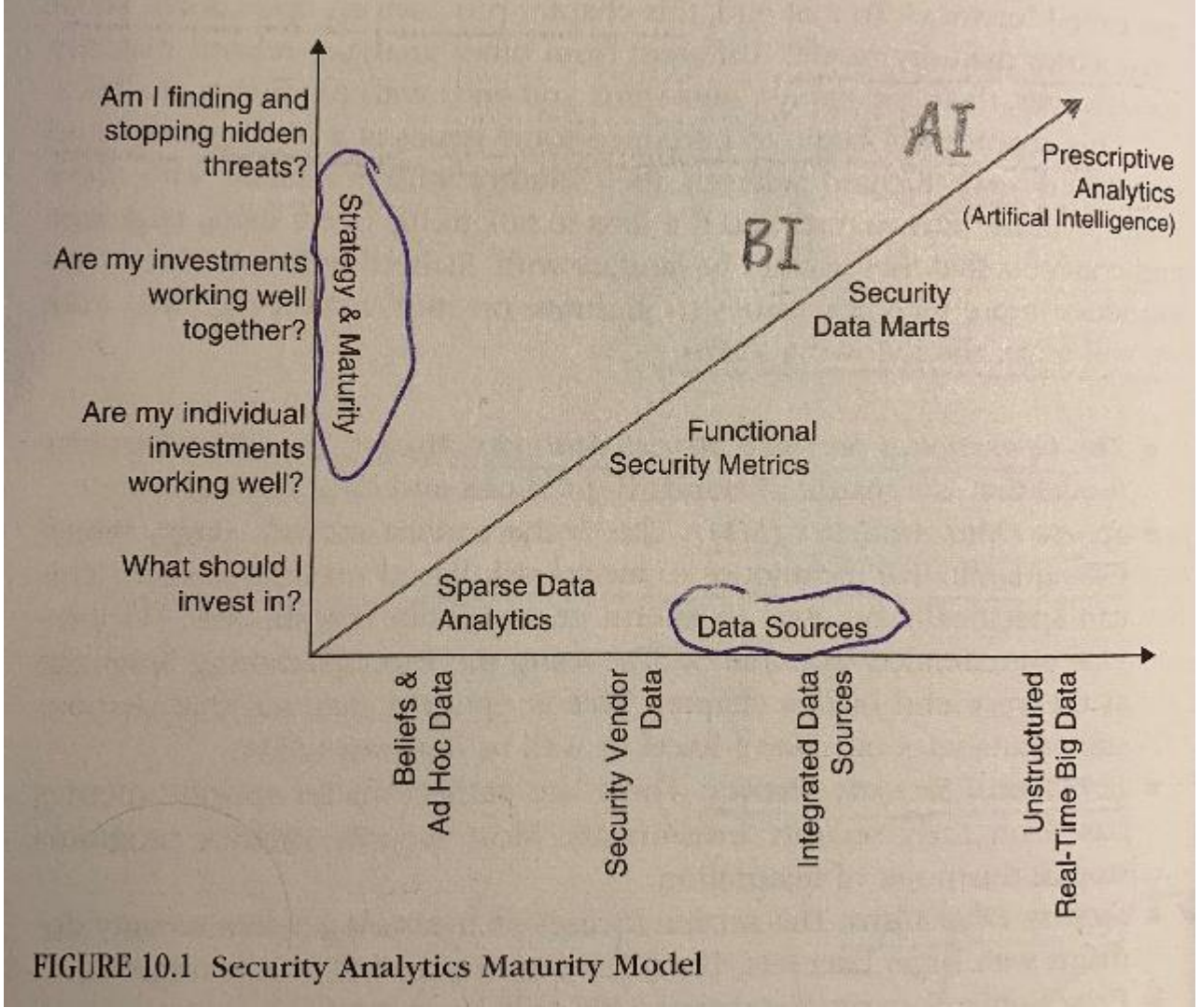


FIGURE 10.1 Security Analytics Maturity Model

ISO 31000:2018

- SS-ISO/IEC 27005:2018

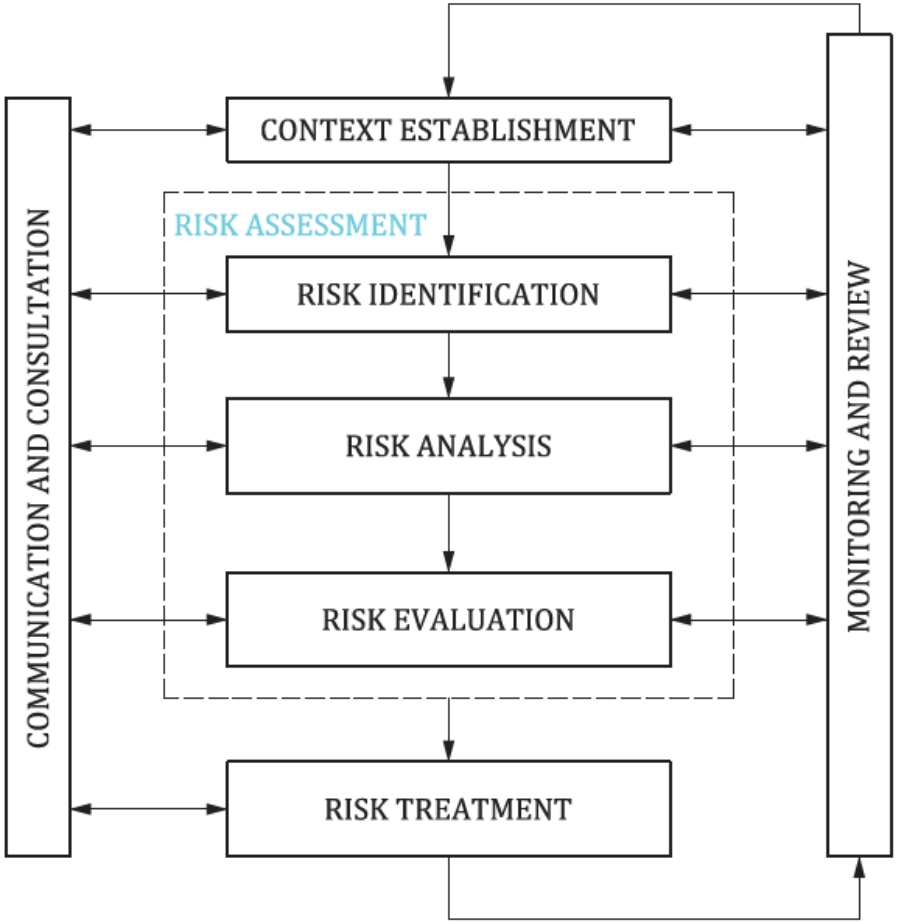


Figure 1 The risk management process

BOKENS HUVUDBUDSKAP

- Analysen ska ge beslutsunderlag

”Byt matrisen mot Excel idag!”

ALTERNATIVA INFÖRANDEN

- Snabba vägen
  - Byt idag!
- Försiktiga vägen
  - Utvärdera ny metodik, planera införande
- Smarta vägen
  - Gör parallella analyser, jämför!
  - Låt oss se ett exempel…

Dokumentunderlag

MEDYTEKK.pdf

Läkemedelsbolag, 100 anst., ny IT-lösning

200122 - Information inför test av två metoder för riskanalys v2.1.docx

Testsyfte, läsanvisningar
Ytterligare förutsättningar
Risklista (8 risker)

Avsnittet 'Riskanalys' enligt informationssäkerhet.se 191228.pdf

Från www.informationssäkerhet.se

Riskbedömningar för båda metoderna 200122 v1.1.xlsx

Sammanställning av riskbedömningar för 8 risker

Douglas Hubbards risk-Excel 2--200122 v0.1.xlsx

Kvantitativa analysresultatet

Resultatsammanställning - 200209 - v2.0.pptx

1) ”Vanliga matrisen”
2) Matrisvy + förlustkurvor

Förtydligade skalor

~~Skalor från MSB:s metod~~		**"Sannolikhet per år"**
~~4 = Mycket hög sannolikhet~~	~~4 = Allvarlig~~	75 -- "3 av 4 år eller oftare"
~~3 = Hög sannolikhet~~	~~3 = Betydande~~	50 – "vartannat år"
~~2 = Medelhög sannolikhet~~	~~2 = Måttlig~~	10 – "var tionde år"
~~1 = Låg sannolikhet~~	~~1 = Försumbar~~	5 – "var tjugonde år eller mer sällan"

Allvarlig	Över 25 miljoner kronor eller avvikelse på över 10% av budgeterad omsättning
Betydande	5 – 25 miljoner kronor eller avvikelse på upp till 10% av budget
Måttlig	1 – 5 miljoner kronor eller avvikelse på upp till 2% av budget
Försumbar	Försumbart eller upp till 1 miljon kronor

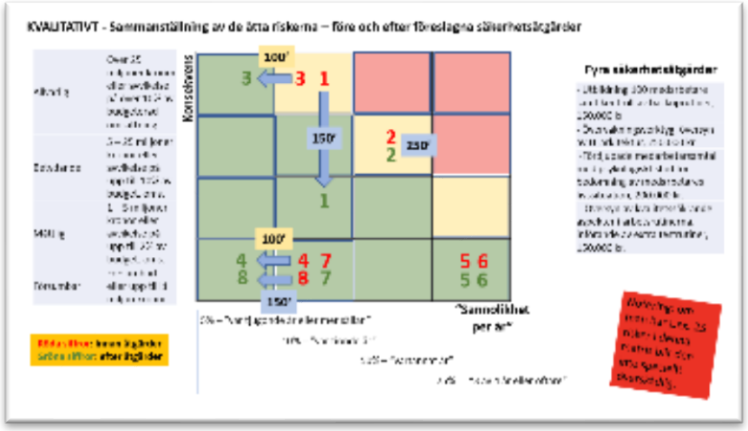
Kvalitativa analysen

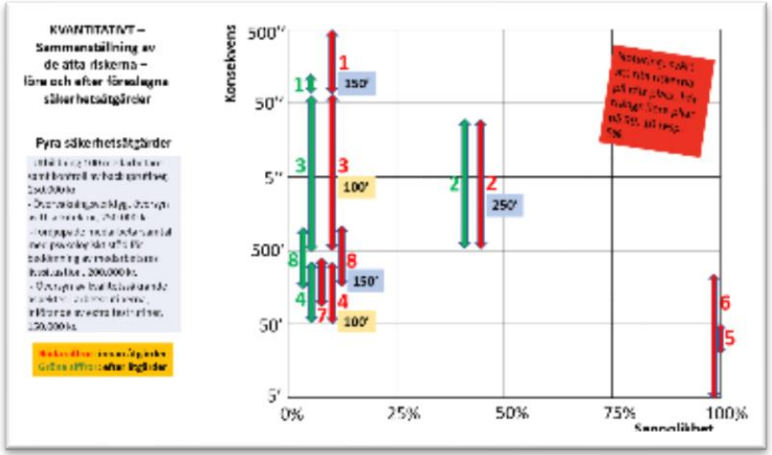
	KVALITATIVT (1)			KVALITATIVT (2)	
Hotlista	Sannolikhet	Konsekvens	Åtgärd	Sannolikhet	Konsekvens
Phishingmejl med ransomware, krypterar alla servrars information, inkl. användbara backuper (kan ej betala sig ur problemet)	2	4	Utbildning 100 medarbetare samt kontroll av backuprutiner, 150.000 kr	2	2
Hackerangrepp, företagets databaser A, B och C eller företagets analysverktyg XYZ kopieras och stjäls (inga personuppgifter)	3ish	3	Övervakningsverktyg, översyn av IT-arkitektur, 250.000 kr	3ish	3
Insiderangrepp, verktyg och databaser kopieras och stjäls	2	4	Fördjupade medarbetarsamtal med psykologiskt stöd för bedömning av medarbetares livssituation, 200.000 kr.	1	4
Insiderangrepp i ekonomisystemet, förskingring av pengar (200.000 kr)	2	1	Samma som ovan.	1	1
Stöld av forskares bärbara dator, ej backup sista veckan	4	1		4	1
Överbelastningsattack (DDoS) under ett dygn	4	1		4	1
Strömavbrott under ett dygn (vardag, ej helg)	2	1		2	1
Felaktig uppdatering av programvara skapar driftstopp två dygn (vardagar, ej helg)	2	1	Översyn av kvalitetssäkrande aspekter i arbetsrutinerna, införande av extra testrutiner, 150.000 kr.	1	1

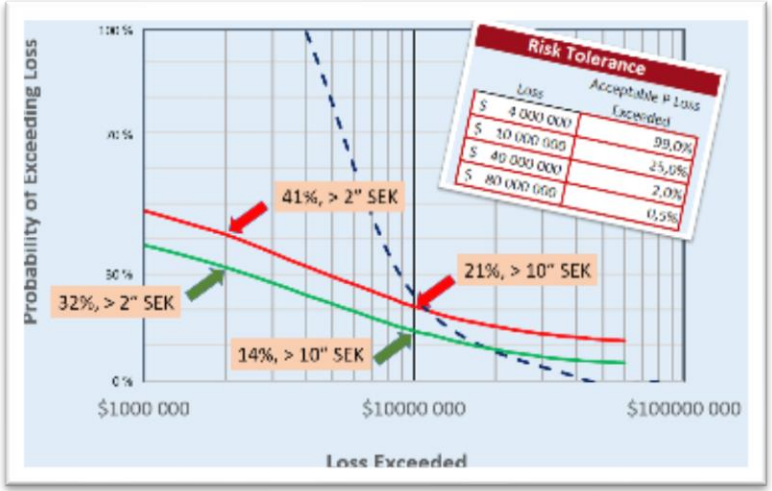
Kvantitativa analysen

	KVANTITATIVT				
Hotlista	Sannolikhet	Konsekvens, låg	Konsekvens, hög	Sannolikhetsminskning efter åtgärd	Konsekvensminskning
Phishingmejl med ransomware, krypterar alla servrars information, inkl. användbara backuper (kan ej betala sig ur problemet)	10%	100''	500''	50%	95%
Hackerangrepp, företagets databaser A, B och C eller företagets analysverktyg XYZ kopieras och stjäls (inga personuppgifter)	40	500'	40''	10%	0%
Insiderangrepp, verktyg och databaser kopieras och stjäls	10	500'	100''	50%	0%
Insiderangrepp i ekonomisystemet, förskingring av pengar (200.000 kr)	10	50'	250'	50%	0%
Stöld av forskares bärbara dator, ej backup sista veckan	99	25'	50'	0%	0%
Överbelastningsattack (DDoS) under ett dygn	99	5'	200'	0%	0%
Strömavbrott under ett dygn (vardag, ej helg)	10	100'	400'	0%	0%
Felaktig uppdatering av programvara skapar driftstopp två dygn (vardagar, ej helg)	10	200'	1''	50%	0%

Jämförelse


KVALITATIVT - Sammanställning av de åtta riskerna – före och efter föreslagna säkerhetsåtgärder
Konsekvens
"Sannolikhet per år"
Fyra säkerhetsåtgärder

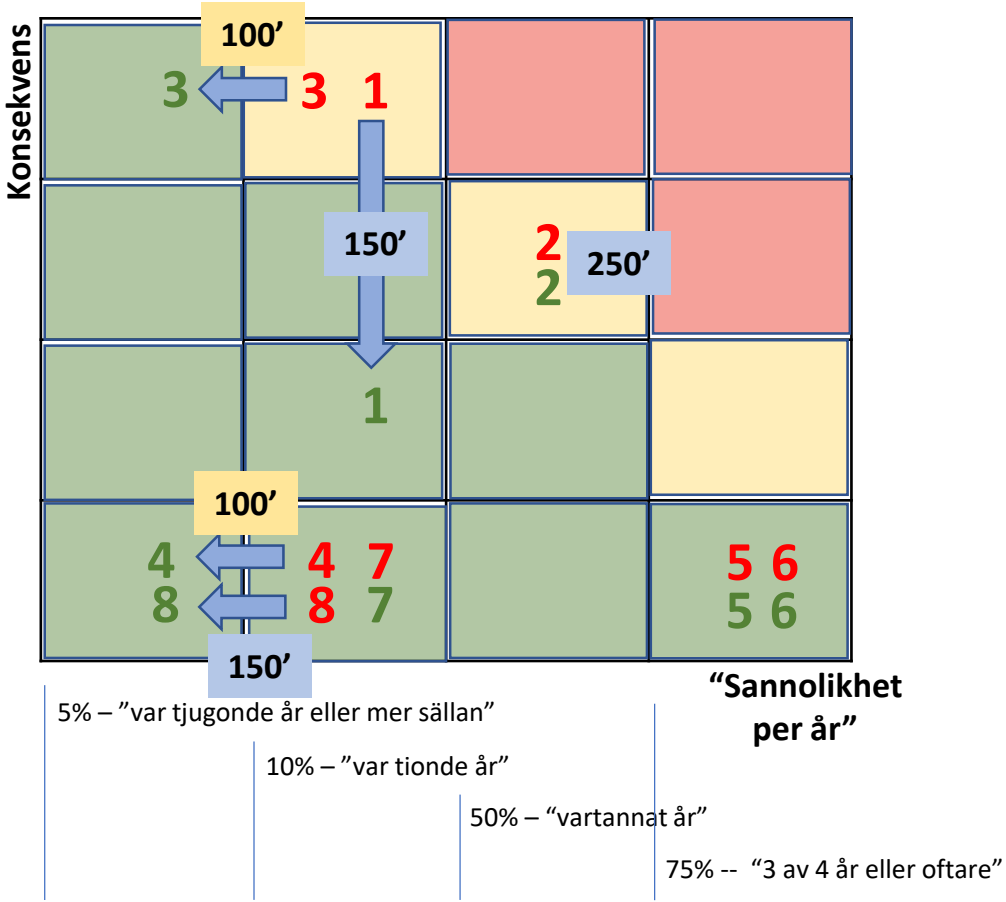

KVANTITATIVT – Sammanställning av de åtta riskerna – före och efter föreslagna säkerhetsåtgärder
Fyra säkerhetsåtgärder
Konsekvens
Sannolikhet


Risk Tolerance
Loss
Acceptable P Loss Exceeded
$ 4 000 000
99,0%
$ 10 000 000
25,0%
$ 40 000 000
2,0%
$ 80 000 000
0,5%
41%, > 2" SEK
32%, > 2" SEK
21%, > 10" SEK
14%, > 10" SEK
Probability of Exceeding Loss
$1000 000
$10000 000
$100000 000
Loss Exceeded

KVALITATIVT - Sammanställning av de åtta riskerna – före och efter föreslagna säkerhetsåtgärder

Allvarlig	Över 25 miljoner kronor eller avvikelse på över 10% av budgeterad omsättning
Betydande	5 – 25 miljoner kronor eller avvikelse på upp till 10% av budget. oms.
Måttlig	1 – 5 miljoner kronor eller avvikelse på upp till 2% av budget. oms.
Försumbar	Försumbart eller upp till 1 miljon kronor

Röda siffror: innan åtgärder
Gröna siffror: efter åtgärder



Fyra säkerhetsåtgärder

- Utbildning 100 medarbetare samt kontroll av backuprutiner, 150.000 kr
- Övervakningsverktyg, översyn av IT-arkitektur, 250.000 kr
- Fördjupade medarbetarsamtal med psykologiskt stöd för bedömning av medarbetares livssituation, 200.000 kr.
- Översyn av kvalitetssäkrande aspekter i arbetsrutinerna, införande av extra testrutiner, 150.000 kr.

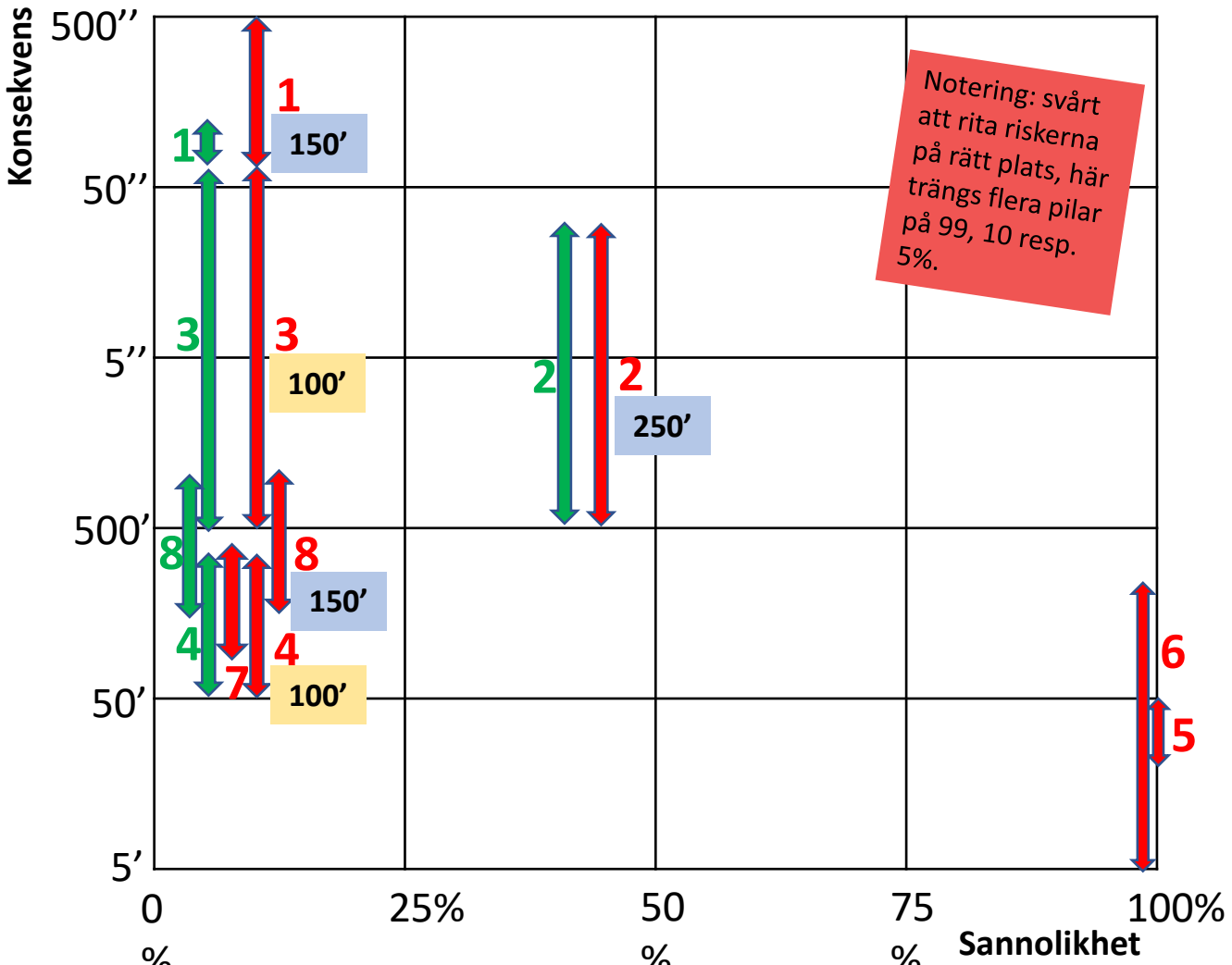
Notering: om man har t.ex. 25 risker i denna matris blir den inte speciellt överskådlig.

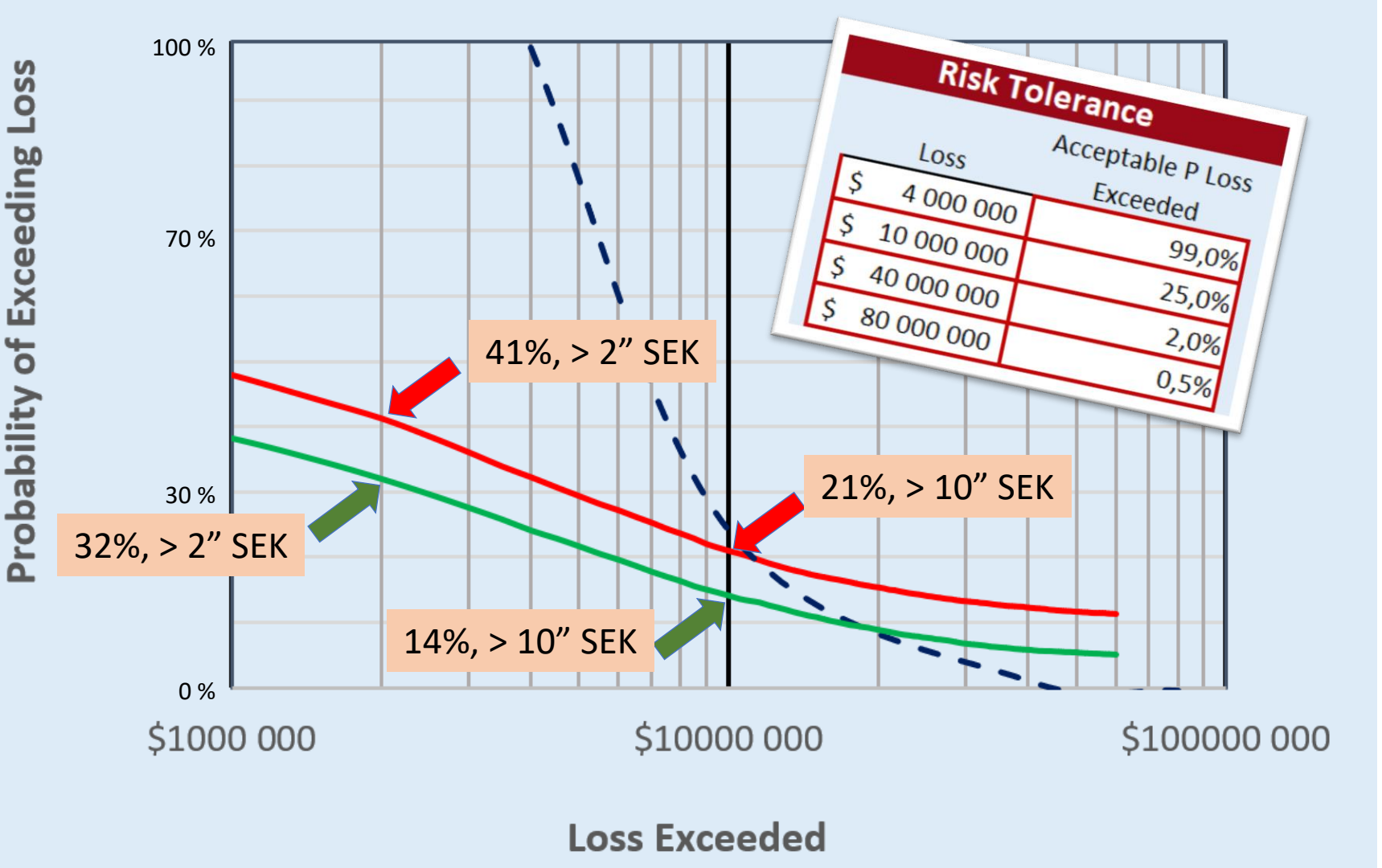
KVANTITATIVT – Sammanställning av de åtta riskerna – före och efter föreslagna säkerhetsåtgärder

Fyra säkerhetsåtgärder

- Utbildning 100 medarbetare samt kontroll av backuprutiner, 150.000 kr
- Övervakningsverktyg, översyn av IT-arkitektur, 250.000 kr
- -Fördjupade medarbetarsamtal med psykologiskt stöd för bedömning av medarbetares livssituation, 200.000 kr.
- - Översyn av kvalitetssäkrande aspekter i arbetsrutinerna, införande av extra testrutiner, 150.000 kr.

Röda siffror: innan åtgärder
Gröna siffror: efter åtgärder




Probability of Exceeding Loss
100 %
70 %
30 %
0 %
$1000 000
$10000 000
$100000 000
Loss Exceeded
41%, > 2” SEK
32%, > 2” SEK
21%, > 10” SEK
14%, > 10” SEK
Risk Tolerance
Loss
Acceptable P Loss Exceeded
$ 4 000 000
99,0%
$ 10 000 000
25,0%
$ 40 000 000
2,0%
$ 80 000 000
0,5%

Alternativa införanden

- Snabba vägen
  - Byt idag!
- Försiktiga vägen
  - Utvärdera ny metodik, planera införande
- Smarta vägen
  - Gör parallella analyser, jämför!

AGENDA

- Riskanalys
  - Boken
  - Problem idag
  - En bättre metod
    - Monte Carlo!
    - Demo
  - Hur införa i organisationen?
  - Frågor och diskussion

TACK FÖR ORDET!

Martin Bergling

martin.bergling@ri.se

070-982 4730