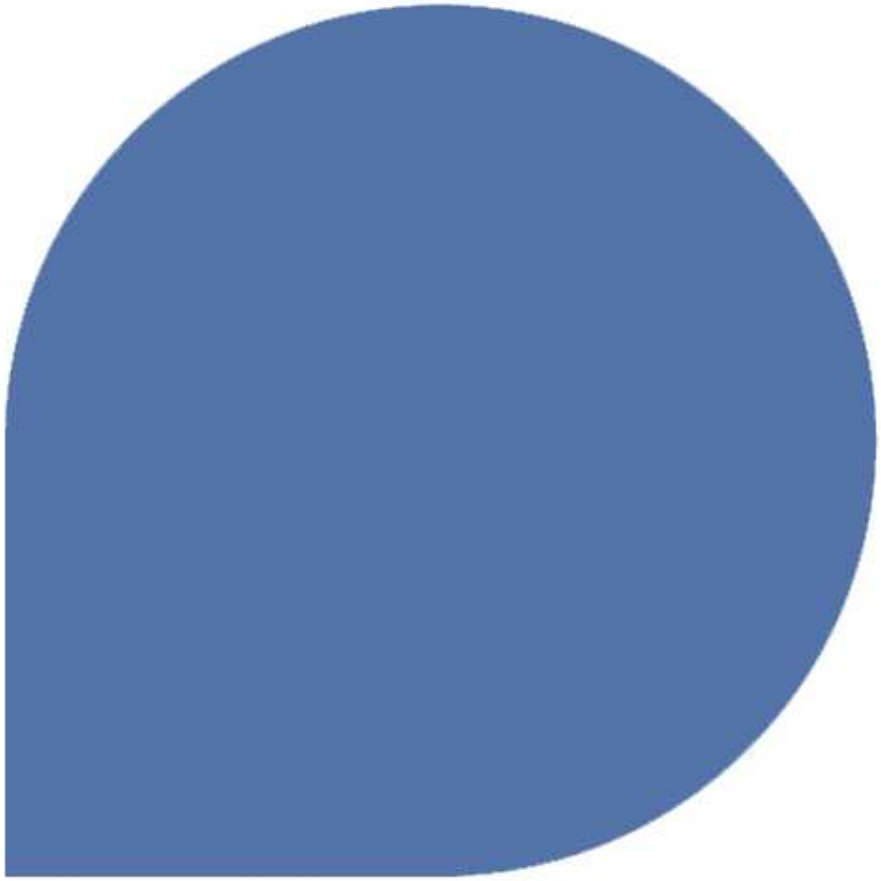
IT-sikkerhet i næringslivet - erfaringer fra bank

Erik Lindmo, DnB

mars 11, 2003



IT er nervesystemet i DnB
- derfor var vi tidlig opptatt av datasikkerhet

- **Betalingsformidling**
  - Håndteres i mange ledd – alltid "men in the middle"
- **Oppbevaring av publikums penger**
  - Må kunne stole på at det er riktig
- **Store transaksjonsvolum**
  - Samfunnskritisk virksomhet
- **Selvbetjening på nett**
  - Sikker autentisering/autorisering

Hvor alvorlig kan det bli ?

- **Ekstra arbeid, frustrasjon**
- **Enkeltkunder utsettes for feil behandling**
- **Negativ mediaomtale**

Hvor alvorlig kan det bli ?

- **Ekstra arbeid, frustrasjon**
- **Enkeltkunder utsettes for feil behandling**
- **Negativ mediaomtale**

- **Feil i forhold til lover/regler**
- **Massekrav fra kunder, rettsaker**
- **Virksomheten blir ulønnsom**
- **Må stoppe bankens drift i en periode**

Hvor alvorlig kan det bli ?

- **Ekstra arbeid, frustrasjon**
- **Enkeltkunder utsettes for feil behandling**
- **Negativ mediaomtale**

- **Feil i forhold til lover/regler**
- **Massekrav fra kunder, rettsaker**
- **Virksomheten blir ulønnsom**
- **Må stoppe bankens drift i en periode**

- **Vansker med å komme i gang igjen**
- **Rot i bankens verdier**
- **Rot i publikums og næringslivets penger som vi oppbevarer og formidler**

Utfordringene underveis

- **Dynamisk teknologi utvikling – gir nye hull**
  - Stormaskin, pc, LAN, selvbetjening, internett, trådløse nett
- **Hvor sikre er vi til enhver tid**
  - Hvordan kan vi vite, måle, fange opp når noe skjer
- **Riktig balanse mellom sikkerhet og kostnader**
  - Høy sikkerhet koster mye – press på kostnader
- **Sikkerheten avhenger av de svakeste ledd**
  - Hvordan skape en kultur slik at alle tenker nok på sikkerhet
- **Dialog med toppledelsen om IT- risiko**
  - i et språk som de forstår – så de kan gi oss riktige føringer

Hva har **vi** gjort

- **"Basis sikkerhetskrav"**
  - interne spilleregler for arbeidet med IT-sikkerhet
- **Bygget It-sikkerhet inn i IT-prosessene**
  - Beslutning, systemutvikling, prod.setting, drift, outsourcing,utfasing, Internkontroll
- **Benchmarking av IT-sikkerhet (ESF)**
  - Hvor god er sikkerheten ift andre internasjonale banker/bedrifter
  - Hvilke forhold har størst betydning for sikkerhet i praksis
  - Nye trusler som oppstår
- **Dialog med ledelsen**
  - Del av deres risikostyring, kostnadskonsekvenser, signaleffekt
- **Se nytten i eksterne krav**
  - IT-forskrifter, EBN/CLS, 2000, BASEL II

BSK – Basis sikkerhetskrav

- **Klassifisering av systemer og data**
- **Roller og ansvar**
- **Personell**

- **Kunder**
- **Tilgangskontroll**
- **Log og sporbarhet**

- **Kryptering**
- **Transport av informasjon**
- **Integritet i basis hw/sw og nettverk**

- **Anskaffelse, systemutvikling og forvaltning Endringskontroll**
- **Drift/produksjon**

- **Fysisk sikkerhet**
- **Back-up**
- **Katastrofeplaner**

- **Forsikring**

- **Etterlevelse av kravene**

Bygget It-sikkerhet inn i IT-prosessene

- **Det er dyrt å tenke sikkerhet "etterpå"**
- **Roller og ansvar i en stor it-organisasjon**
  - Oppdragsgiver,utvikler, platform,drift, nettverk, sikkerhetsavd..
- **"Forretningsmesssige behov for it-sikkerhet"**
  - del av beslutningsgrunnlaget for nye systemer
- **Sikkerhetsanalyse**
- **Ved Produkjonssetting må alt være klart**
- **Endringskontroll**
- **"The incremental risk"**

DnB

Benchmarking av IT-sikkerhet (ISF)

- **Benchmarking 2.hvert år**
  - - 250 sikkerhetsbevisste internasjonale bedrifter
  - Detaljerte spørreskjema – 1.000 + spørsmål
  - Rapporterer også major incidents og konsekvenser

- **Resultat:**
  - Status ift forrige gang
  - (totalt, platformer,forretningskritiske applikasjoner, nettverk, sys.utvikling/forvaltning, sikkerhetsavdelingen)
  - Status ift sammenlignbare bedrifter, miljøer
  - Incidents, frekvens og konsekvenser
  - **Key factors** for effektiv sikkerhet

Findings…

- **Mangelfull sikkerhet koster:** reduserer overskudd 2-3 % (gj.snitt)
- **Mest å hente på :** å sikre tilgjengelighet
- **Største trussel:** "things going wrong" (unintentionally)
- **Mange små hendelser:** 10 hver dag - 4.200 pr år (gj.snitt)
- **Major incidents:** sannsynligvis 1 gang pr. år (gj.snitt)
- **Årsak til hendelser:** som regel internt, dvs under bedriftens egen kontroll

Kan noe gjøres ?

- **Benchmark miljøer har redusert "cost of insecurity til 1/3 – ¼**

- **47 key factors identifisert** disse bidrar mest til å redusere tap/skade
  = de mest effektive sikkerhetstiltak

Disse 47 key faktorene kan grupperes i..

- **Comitment from top**
- **Individual accountability** **= good management**
- **Disciplined relationships**

- **Systematic assesments of risk**
- **Know how development** **= active driving force**
- **Sound rules**
- **Independant reviews**

- **Establish a sound environment**
- **Get operational things right**
- **Discipline the handling of changes** **= sound basic practices**
- **Control access to system capabilities**
- **Control othjer obvious risks**

Spesielle utfordringer ved e-handel/selvbetjening ?

- **Leverandør/tjeneste siden**
  Alle vanlige IT-sikkerhetsproblemer +
  Spes.urfordringer: Tilgjengelighet, hyppige produksjonsendringer, "systemet" består av mange komponenter, katastrofeløsninger

- **Transaksjoner**
  - Sikker autentisering, sikret mot endring, benekting (PKI ?)

- **Kundesiden**
  - Mange ulike konfigurasjoner "der ute",
  - krav til installering, hyppige endringer
  - Brukervennlighet - kundeservice

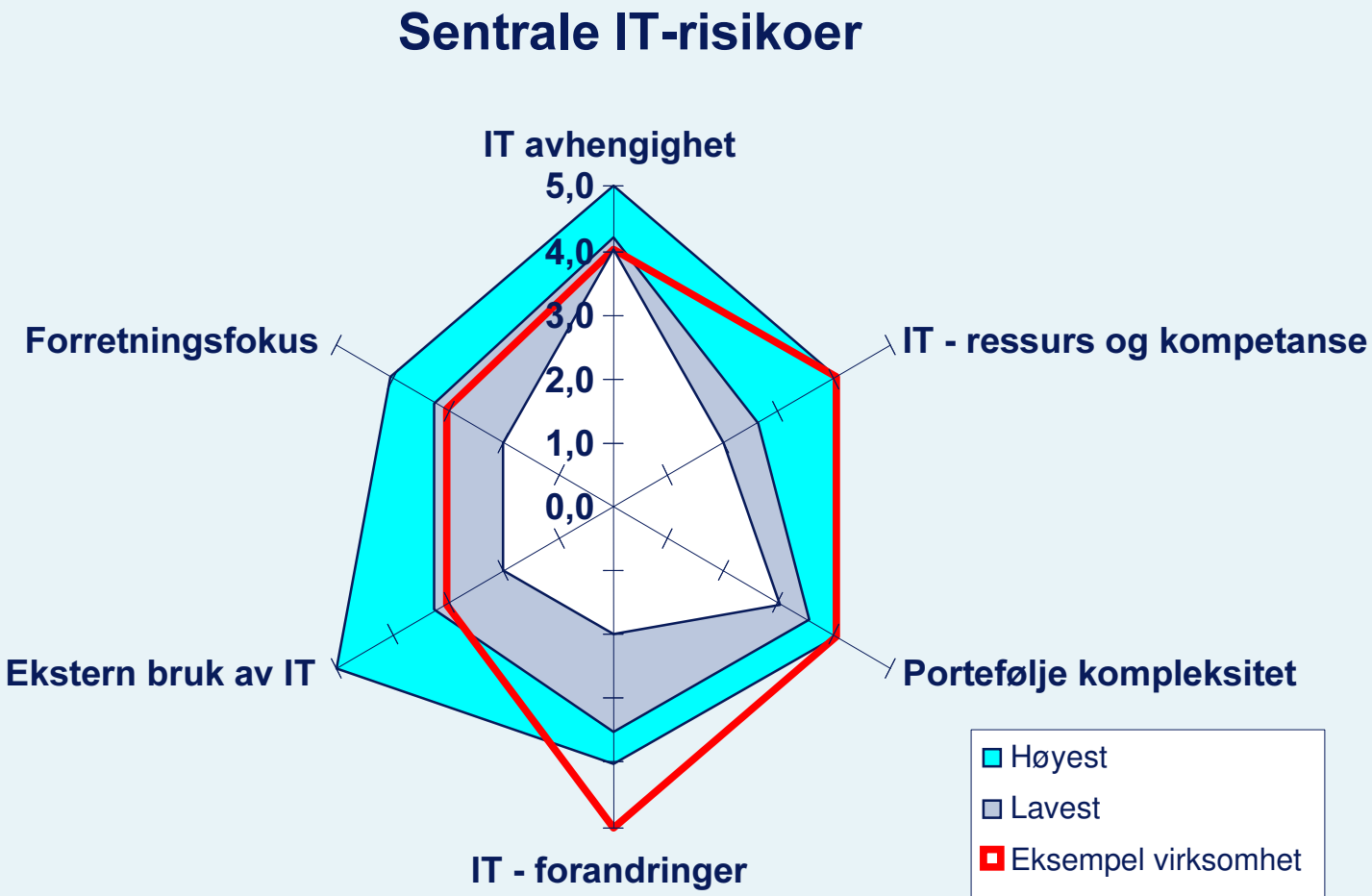
- **Lover og regler**
  - Elektroniske dokumenter, signaturer
  - Privacy, personvern

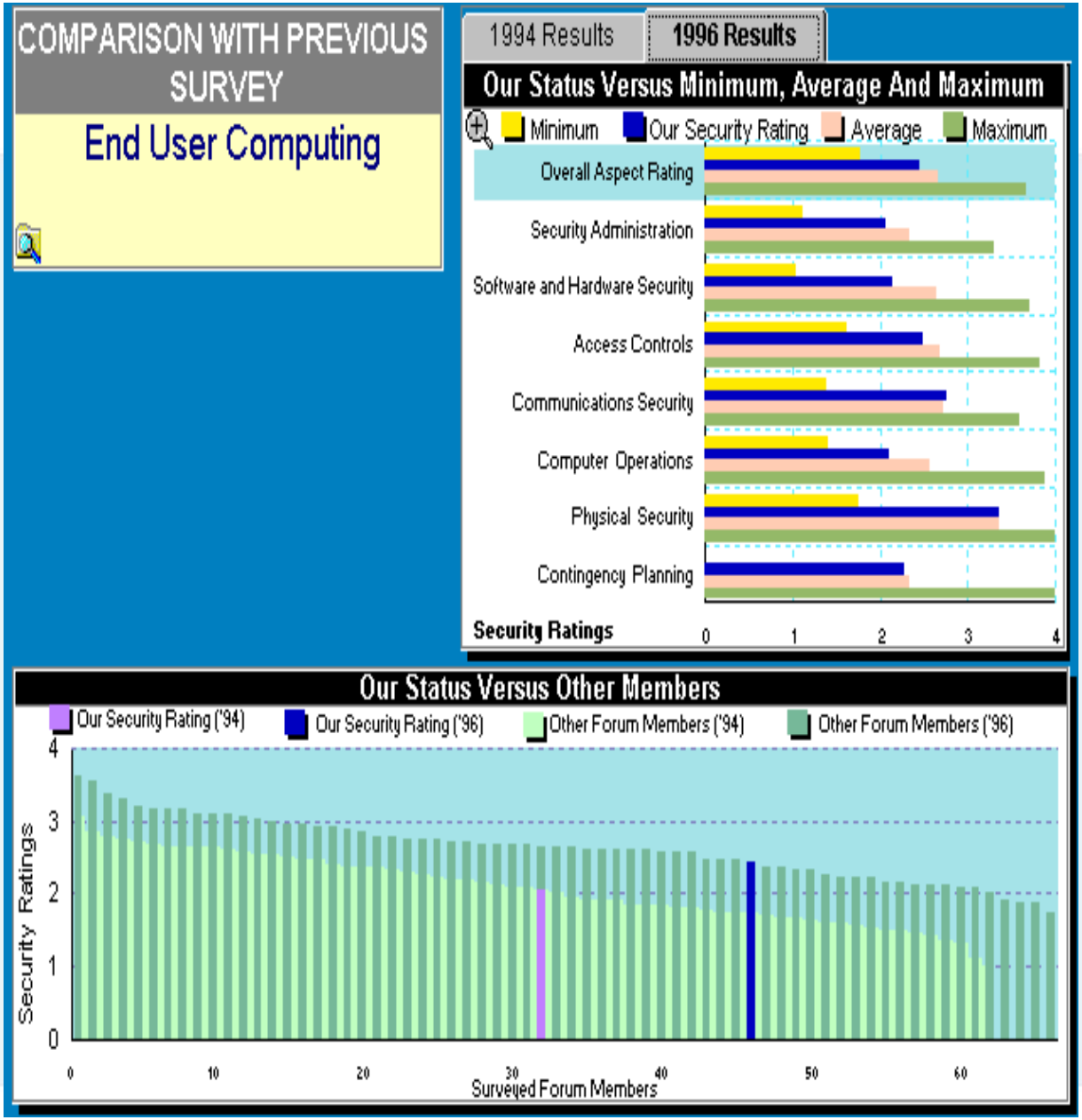
Dialog med ledelsen

- **ledelsen er opptatt av:**
  - kroner
  - risiko
  - hva gjør de andre
  - renommé
  - følge lover

- **It-sikkerhet er for teknisk – hvordan forklare ?**
  - Grafisk
  - Analogier fra den fysiske verden

Et tenkt eksempel..




COMPARISON WITH PREVIOUS SURVEY
End User Computing
1994 Results
1996 Results
Our Status Versus Minimum, Average And Maximum
Minimum
Our Security Rating
Average
Maximum
Overall Aspect Rating
Security Administration
Software and Hardware Security
Access Controls
Communications Security
Computer Operations
Physical Security
Contingency Planning
Security Ratings
0
1
2
3
4
Our Status Versus Other Members
Our Security Rating ('94)
Our Security Rating ('96)
Other Forum Members ('94)
Other Forum Members ('96)
Security Ratings
0
1
2
3
4
0
10
20
30
40
50
60
Surveyed Forum Members

Se nytten i eksterne krav

- **It-forskriftene og kreditt-tilsynets oppfølging**
- **Intern-kontroll**
- **Krav fra Internasjonale bank-systemer**
  - SWIFT,CLS

- Nå kommer **Basel II (2006)**
  - EK-krav 8% av utlånsbalansen - dekker kreditrisiko
  - => utvides til å dekke operasjonell risiko

  - Basic indicator - 8 % av 200 mrd
  - Standard method - 3 % x utlån + 5 % x bet.formidl + ….
  - Advanced internal method - (basert på ISF-tenking ?)

  - **Reduksjon av IT-risiko slår direkte ut på EK-kravet**
  - **- et språk som ledelsen forstår**

Nyttige linker:

http://securityforum.org

http://www.bis.org