FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

Seminar 23. mai 2013

Risiko- og sårbarhetsanalyse (ROS) 2012
Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi

Seksjonssjef Frank Robert Berg

ROS-analysen 2012:

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Kap. 1) Innledning – sammendrag
- Kap. 2) Utviklingstrekk
  - Trender som kan påvirke risiko
- Kap. 3) Risiko knyttet til tjenestene og tap
- Kap. 4) Funn og observasjoner
  - Bruk av kilder og drøfting av funn
- Kap. 5) Identifiserte risikoområder
  - Spesielle fokus- og tiltaksområder
- Kap. 6) Finanstilsynets oppfølging
  - Hva kan tilsynet gjøre?

Risikobildet og trusselutviklingen 2012

Samarbeid Finanstilsynet – Norges Bank

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Skaffe oss oversikt
- Analysere
- Foreslå tiltak

Leveranse

Årlig ROS-analyse
Risiko
Sikkerhet

- Resultater fra tilsyn – IT og betalingstjenester
- Gjennomførte ROS-intervju
- Hendelseshåndtering – Data fra hendelsesdatabase
- Betalingstjenester – Meldeplikt - Betalings-tjenester
- Annen relevant informasjon spørre-undersøkelser
- Beredskap
  - BFI-sekretariatet
  - Samarbeid andre myndigheter
  - Infrastruktur betalingssystemer

Våre virkemidler

2. Utviklingstrekk

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Privat utstyr – Risiko for å åpne en «bakdør»
- Identitetstyveri
- Utkontraktering
- Tjenesteutvikling i betalingssystemer
- Regulatoriske utviklingstrekk
- Internasjonal utvikling
- Felles tiltak fra finansnæringen

2. Utviklingstrekk

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Privat utstyr – Risiko for å åpne en «bakdør»
- Identitetstyveri
- Utkontraktering
- Tjenesteutvikling i betalingssystemer
- Regulatoriske utviklingstrekk
- Internasjonal utvikling
- Felles tiltak fra finansnæringen

2. Utviklingstrekk - Identitetstyveri

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- ✓ Det foreligger mange estimater over omfanget av ID-tyveri. Mange av estimatene bygger på spørreundersøkelser.
- ✓ Reelle tapstall fra ID-tyveri innhentet av FNO, i samarbeid med Finanstilsynet, angir tap i finanssektoren i 2012 til 7,5 millioner NOK.
- ✓ Tall fra andre nasjoner (USA) viser at dette er et alvorlig problem.
- ✓ Krenkelsen den enkelte blir utsatt for ved ID-tyveri er svært alvorlig.
- ✓ Finanstilsynet samarbeider med Datatilsynet om kartlegging og tiltak.

2. Utviklingstrekk

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

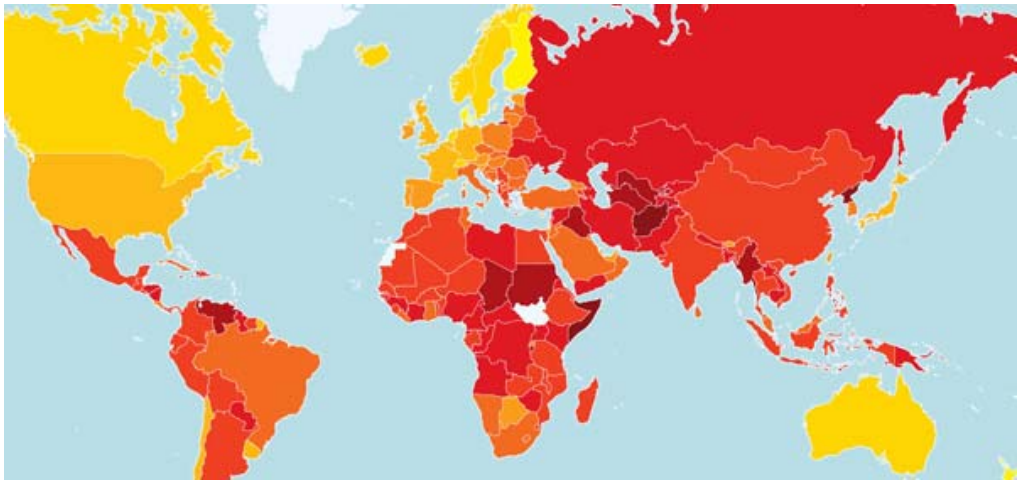
- Privat utstyr – Risiko for å åpne en «bakdør»
- Identitetstyveri
- Utkontraktering
- Tjenesteutvikling i betalingssystemer
- Regulatoriske utviklingstrekk
- Internasjonal utvikling
- Felles tiltak fra finansnæringen

2. Utviklingstrekk - Utkontraktering

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

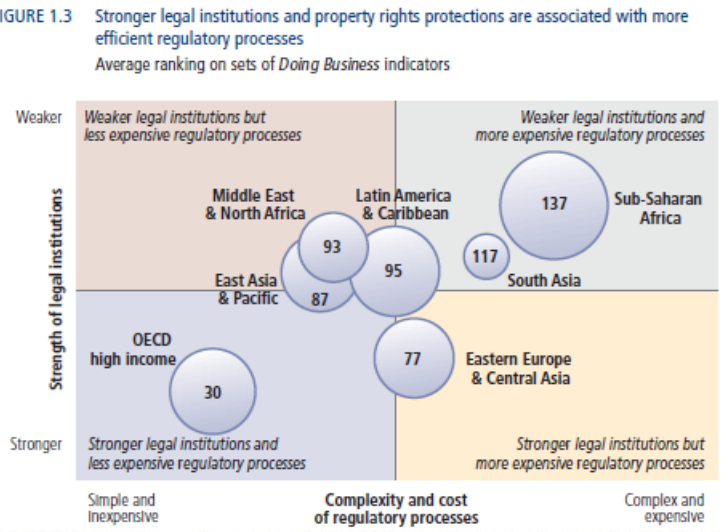
Sikre egen styring og kontroll

Transparency International
The 2012 corruption perceptions index



Doing Business
THE WORLD BANK IFC
2012

Indisk IT under lupen, DN, 21.05.2013



2. Utviklingstrekk

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Privat utstyr – Risiko for å åpne en «bakdør»
- Identitetstyveri
- Utkontraktering
- Tjenesteutvikling i betalingssystemer
- Regulatoriske utviklingstrekk
- Internasjonal utvikling
- Felles tiltak fra finansnæringen

2. Utviklingstrekk - Tjenesteutvikling i betalingssystemer

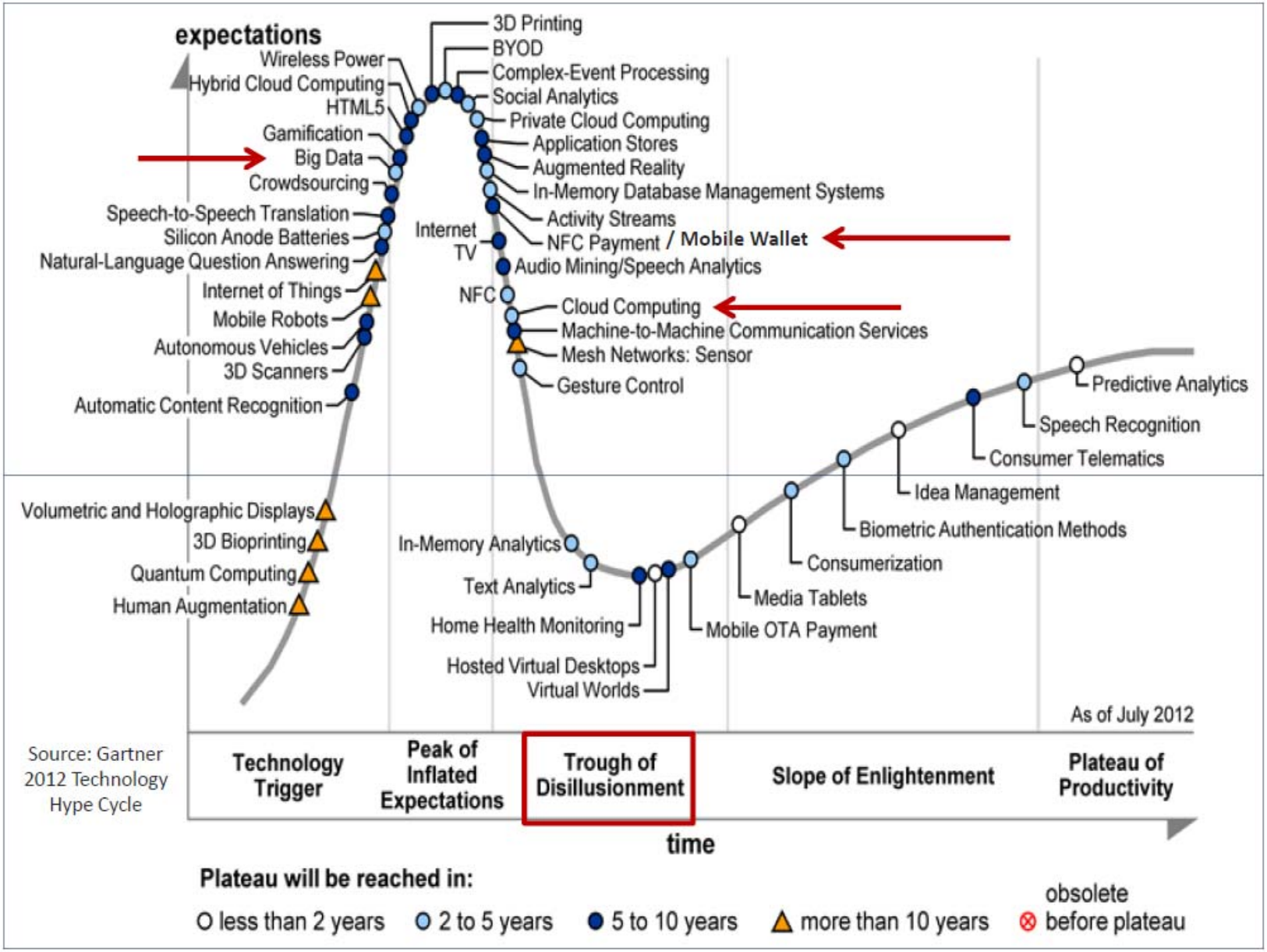
FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Nettet gir unike muligheter for «Betalingstjenester utenfor regulering»:
Pay Pal, TrustBuddy, Popmoney, Bitcoin, Facebook coins, Microsoft points. Andre tjenester: Overlay payment service.

”Technology by itself will not deliver a competitive advantage; what banks do with it to develop a unique, personalized customer experience will matter most of all”

- Bain & Company (2012)

Drivere:
Sosiale medier, nettkapasitet, big data, nettskyer, nye devicer


expectations
3D Printing
BYOD
Complex-Event Processing
Social Analytics
Private Cloud Computing
Application Stores
Augmented Reality
In-Memory Database Management Systems
Activity Streams
NFC Payment / Mobile Wallet
Audio Mining/Speech Analytics
Cloud Computing
Machine-to-Machine Communication Services
Mesh Networks: Sensor
Gesture Control
Wireless Power
Hybrid Cloud Computing
HTML5
Gamification
Big Data
Crowdsourcing
Speech-to-Speech Translation
Silicon Anode Batteries
Natural-Language Question Answering
Internet of Things
Mobile Robots
Autonomous Vehicles
3D Scanners
Automatic Content Recognition
Internet TV
NFC
Predictive Analytics
Speech Recognition
Consumer Telematics
Idea Management
Biometric Authentication Methods
Consumerization
Media Tablets
Mobile OTA Payment
Volumetric and Holographic Displays
3D Bioprinting
Quantum Computing
Human Augmentation
In-Memory Analytics
Text Analytics
Home Health Monitoring
Hosted Virtual Desktops
Virtual Worlds
As of July 2012
Source: Gartner 2012 Technology Hype Cycle
Technology Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity
time
Plateau will be reached in:
less than 2 years
2 to 5 years
5 to 10 years
more than 10 years
obsolete before plateau

2. Utviklingstrekk

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Privat utstyr – Risiko for å åpne en «bakdør»
- Identitetstyveri
- Utkontraktering
- Tjenesteutvikling i betalingssystemer
- Regulatoriske utviklingstrekk - EU som driver
- Internasjonal utvikling
- Felles tiltak fra finansnæringen

2. Utviklingstrekk

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Privat utstyr – Risiko for å åpne en «bakdør»
- Identitetstyveri
- Utkontraktering
- Tjenesteutvikling i betalingssystemer
- Regulatoriske utviklingstrekk
- Internasjonal utvikling - Skytjenester
- Felles tiltak fra finansnæringen

2. Utviklingstrekk

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Privat utstyr – Risiko for å åpne en «bakdør»
- Identitetstyveri
- Utkontraktering
- Tjenesteutvikling i betalingssystemer
- Regulatoriske utviklingstrekk
- Internasjonal utvikling
- Felles tiltak fra finansnæringen – BSK / egenregulering

2. Utviklingstrekk – Felles tiltak

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Hva er en CERT?

FinansCERT

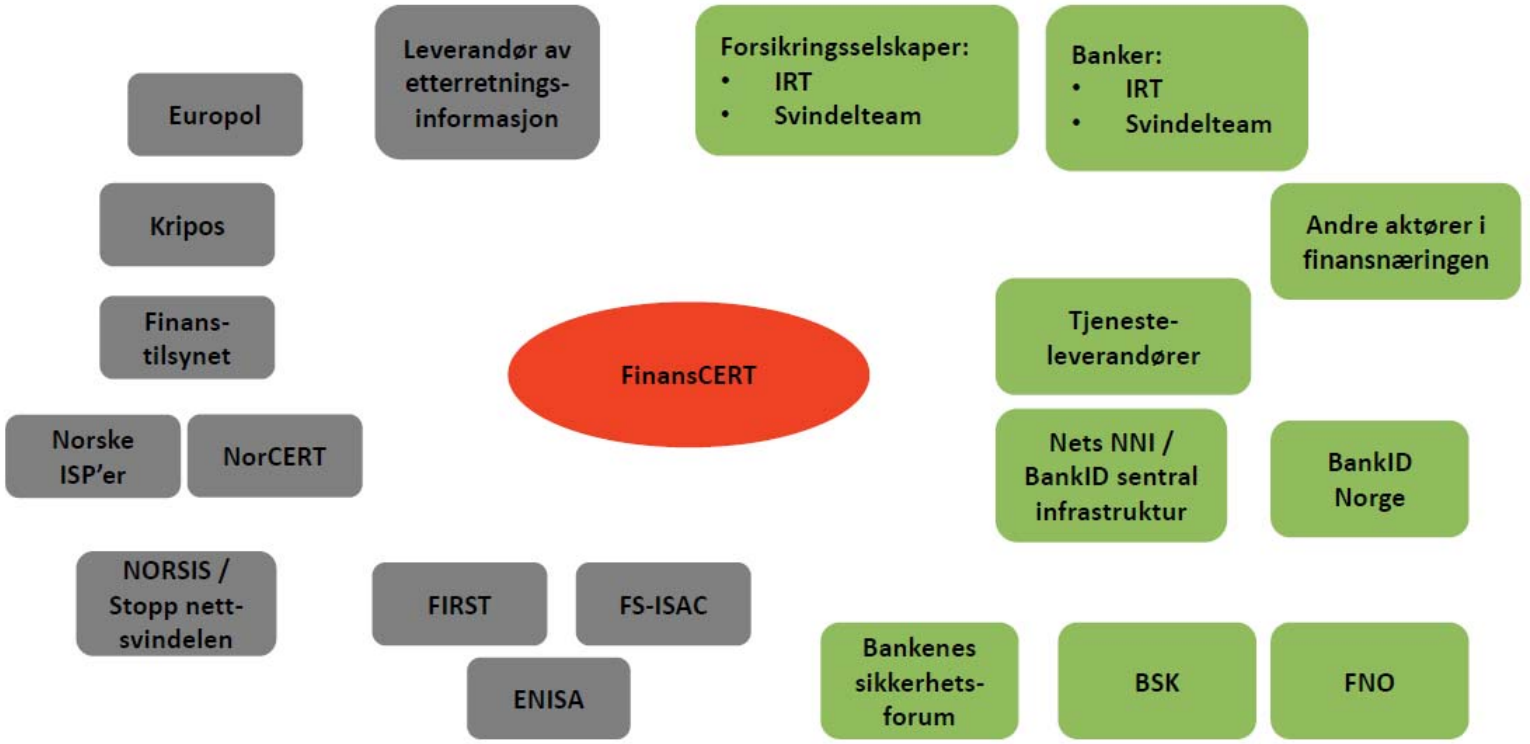
- Computer Emergency Response Team (CERT)
  - Et annet navn på det samme er Computer Incident Response Team (CSIRT)
- Håndterer IT-sikkerhetshendelser, blant annet ved varsling og informasjonsdeling
- I Norge er følgende CERT'er og CSIRT's mest kjent:
  - NorCERT (Nasjonal CERT for samfunnsviktig infrastruktur)
  - Helse CSIRT
  - Justis CSIRT
  - Telenor CERT
  - Uninett CERT

Kilde: FinansCERT

2. Utviklingstrekk – Felles tiltak

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Dialog med eksterne kontaktpunkter vil være sentralt for FinansCERT, under ser man noen mulige samarbeidspartnere:



Kilde: FinansCERT

3. Systemer for betalingstjenester

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Generelt om betalingssystemer
- Styring og kontroll med betalingssystemer
- Risiko og sårbarhet i betalingssystemene
- Oversikt over tap knyttet til betalingstjenester

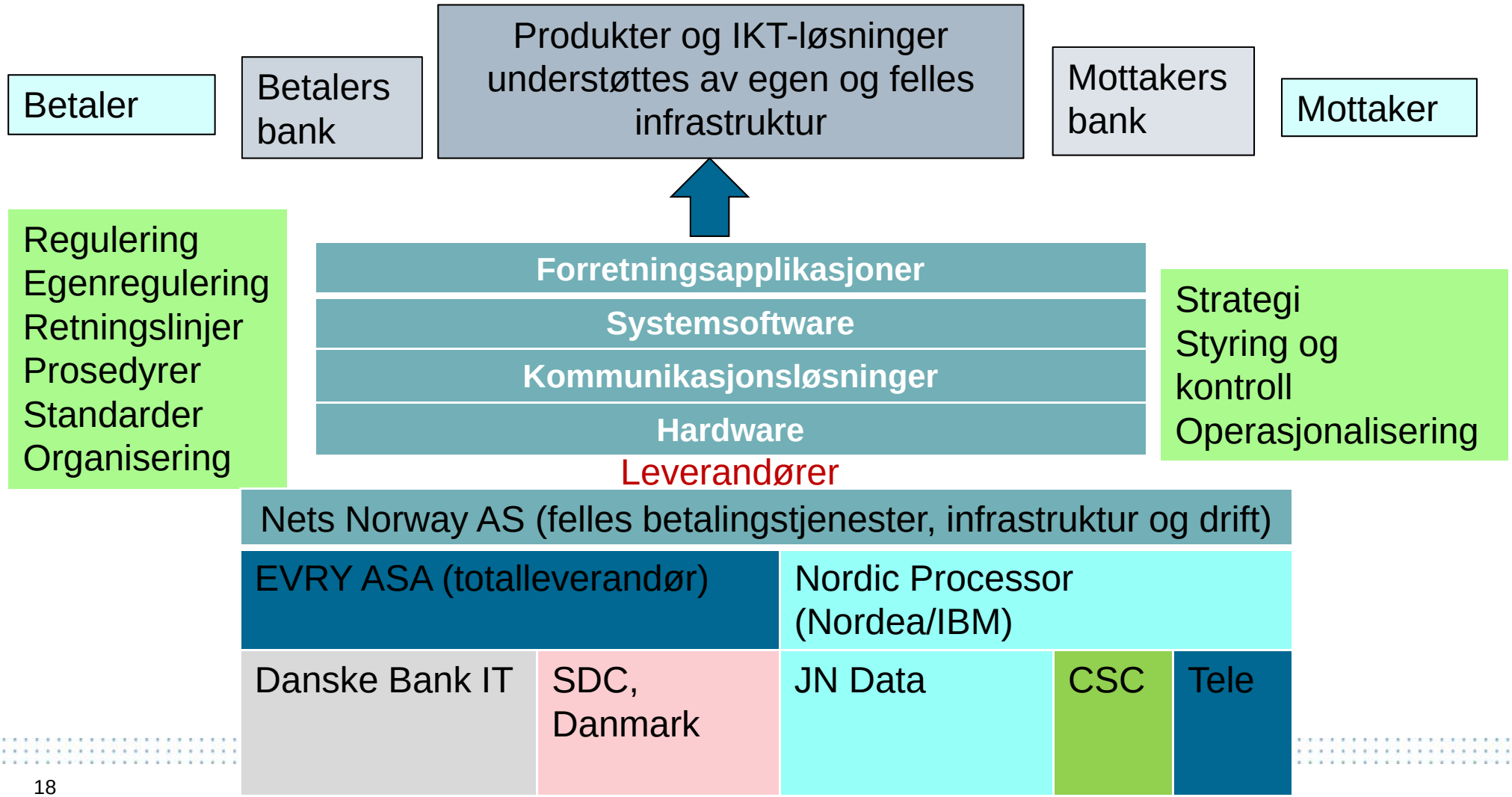
Ikke planlagte hendelser
Manglende styring og kontroll

Planlagte hendelser
Analyse beredskap og tiltak

Betalingssystemer

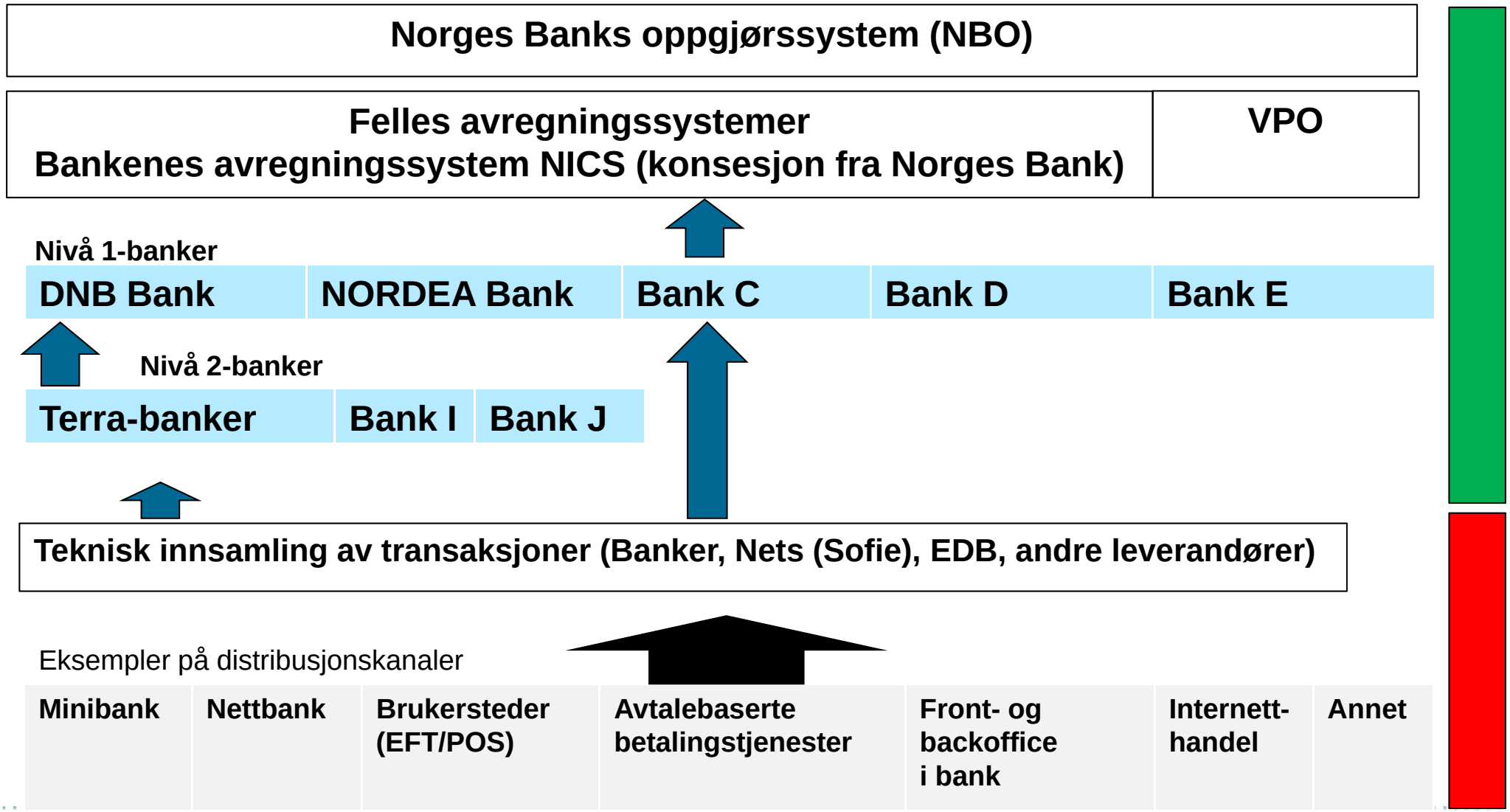
FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Infrastrukturen som understøtter stadig mer avanserte betalingsløsninger, er kompleks:



Logisk og forenklet bilde av transaksjonsflyten fra der den oppstår, innsamling, avregning og oppgjør

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY



Tap i 2012 ved bruk av betalingskort

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Tabell 1: Tap ved bruk av betalingskort (tall i hele tusen kroner)

Svindeltype betalingskort	2011	2012
Misbruk av kortinformasjon, kort ikke til stede (internetthandel)	24 190	35 701
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort i Norge	468	2 308
Stjålet kortinformasjon (inkludert skimming), misbrukt med falske kort utenfor Norge	57 340	55 869
Originalkort tapt eller stjålet, misbrukt med PIN i Norge	32 224	28 128
Originalkort tapt eller stjålet, misbrukt med PIN utenfor Norge	7 008	8 544
Originalkort tapt eller stjålet, misbrukt uten PIN	4 488	4 603
TOTALT	**125 718**	**135 153**

Kilde: Finanstilsynet

Tap i 2012 ved bruk av nettbank

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

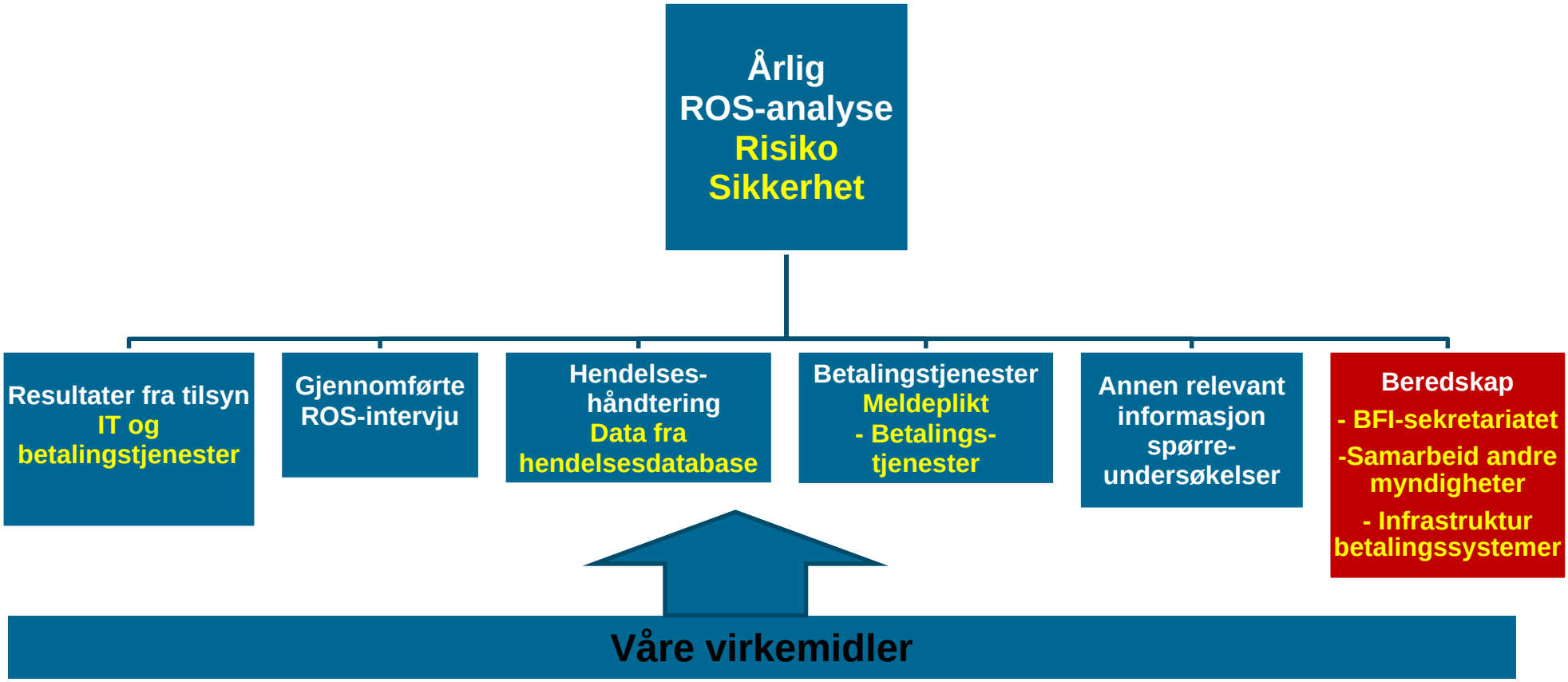
Tabell 2: Tap ved bruk av nettbank (tall i hele tusen kr)

Svindeltype nettbank	2011	2012
Angrep ved bruk av ondartet programkode på kundens PC (trojaner)	664	5 064
Angrep som utnytter sårbarheter i nettbankapplikasjon (hacking)	0	0
Tapt/stålet sikkerhetsmekanisme	3 321	3 367
TOTALT	**3 985**	**8 431**

Kilde: Finanstilsynet

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

4. Funn og observasjoner



Identifiserte risikoområder

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Styring og kontroll
- Angrep på nettbaserte løsninger
- Kontinuitets- og katastrofeløsninger
- Risiko ved gamle og komplekse systemer
- Tilgang til betalingstjenestene

Styring og kontroll

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Nødvendig kunnskap om IT-governance og beste praksis i å styre IKT-virksomheten.
- Det betyr i praksis å etablere rammeverk som omfatter: roller og ansvar, prosessbeskrivelser, rutiner/retningslinjer, bruk av verktøy og kontroll.
- Detaljerte avtaler ved utkontraktering, tydelig forankring av ansvar og system for kontroll av leveransene.

Angrep på nettbaserte løsninger

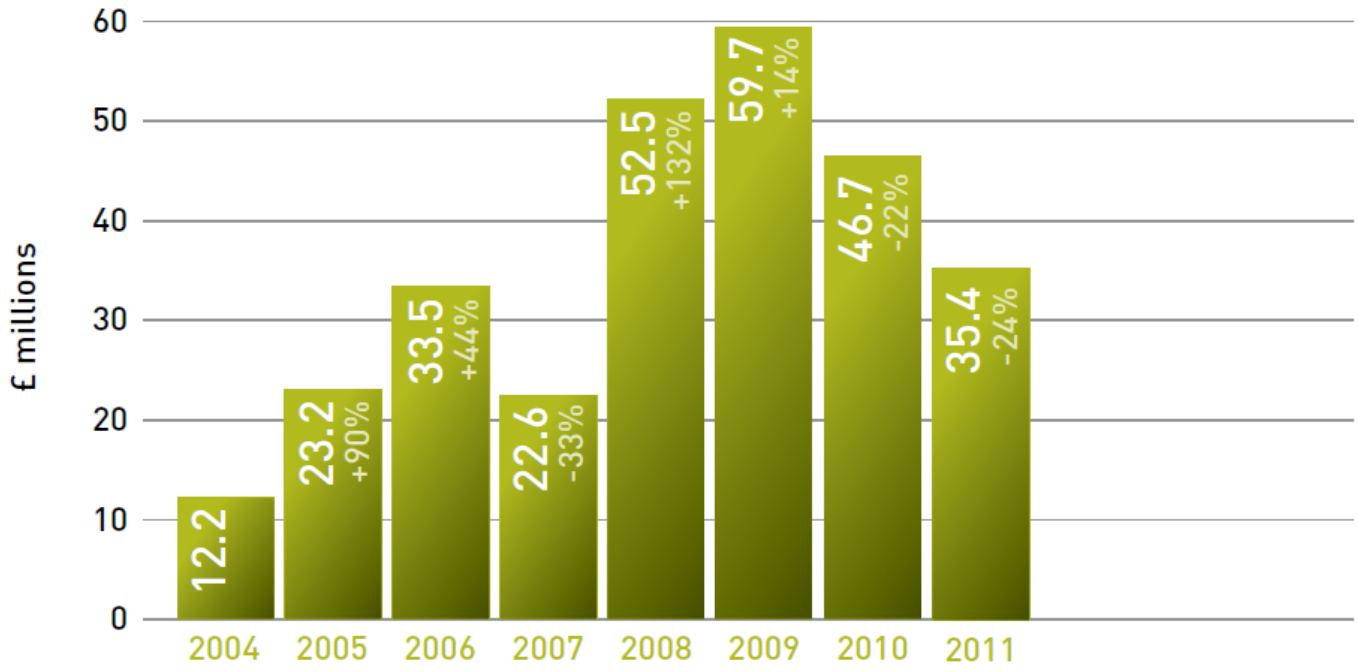
FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Noen ulike roller knyttet til nettbanksvindel

Rolle	Oppgaver
Malware-utvikler	De som forestår den grunnleggende programvareutviklingen.
Rekrutterer muldyr	Sikrer at noen stiller en konto til rådighet i landet som skal angripes.
Muldyr	Den som stiller konto til rådighet og foretar videre overførsler/uttak.
Setter sammen angrepskoden	Skreddersyr angrepet basert på grunnkoden.
Spredning av angrepskoden	Sprer koden gjennom ulike opplegg, f.eks. gjennom reklameannonser eller svakheter i programvare som f.eks. operativsystem eller nettleser.
Utnytter infiserte PC-er	Gjennomfører angrep mot infiserte PC-er gjennom overvåkning og tiltak eller gjennom logikk bygget i koden.
Sikrer mottak av penger	Foretak som utfører pengeoverføringstjenester.

ONLINE BANKING FRAUD LOSSES 2004-2011

Tinted figures show percentage change on previous year's total



Kilde: UK Payment Administration Ltd / Financial Fraud Action UK

NUMBER OF PHISHING WEBSITES* TARGETED AGAINST UK BANKS AND BUILDING SOCIETIES BY MONTH 2005-2011

	Jan	Feb	Mar	Apr	May	June	July	Aug	Sept	Oct	Nov	Dec	TOTAL
2011	5,803	5,757	6,828	5,698	6,216	6,896	7,402	8,062	23,083	9,397	15,395	10,749	111,286
2010	2.654	3,135	4,810	4,335	5,406	5,277	5,873	5,861	5,689	6,977	4,552	7,304	61,873
2009	4,206	5,161	5,004	3,422	3,917	4,335	4,415	4,845	3,900	4,903	4,191	5,864	51,161
2008	3,144	3,243	3,848	3,719	3,091	3,637	3,584	3,716	4,121	4,536	3,896	3,456	43,991
2007	1,290	974	1,130	1,188	1,274	1,368	3,066	3,268	2,597	3,170	3,277	3,195	25,797
2006	606	669	1,074	947	919	872	970	1,484	1,513	1,596	1,993	1,513	14,156
2005	18	29	27	54	72	122	153	160	190	267	255	353	1,700

* Fraudsters set up a website that is a fake version of a genuine bank website, and then send out thousands or even millions of spam emails trying to convince people to click on a link that will send them to that fake site.

Kilde: UK Payment Administration Ltd / Financial Fraud Action UK

Kontinuitets- og katastrofeløsninger

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Kontinuitetsløsninger
- Opplegg for håndtering av hendelser
- Etablering av katastrofeløsning, vedlikehold og testing – verifisering av testresultat
- Risikovurdering av alle elementer som inngår
- Identifisere og sikre kritiske komponenter

Risiko ved gamle og komplekse systemer

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

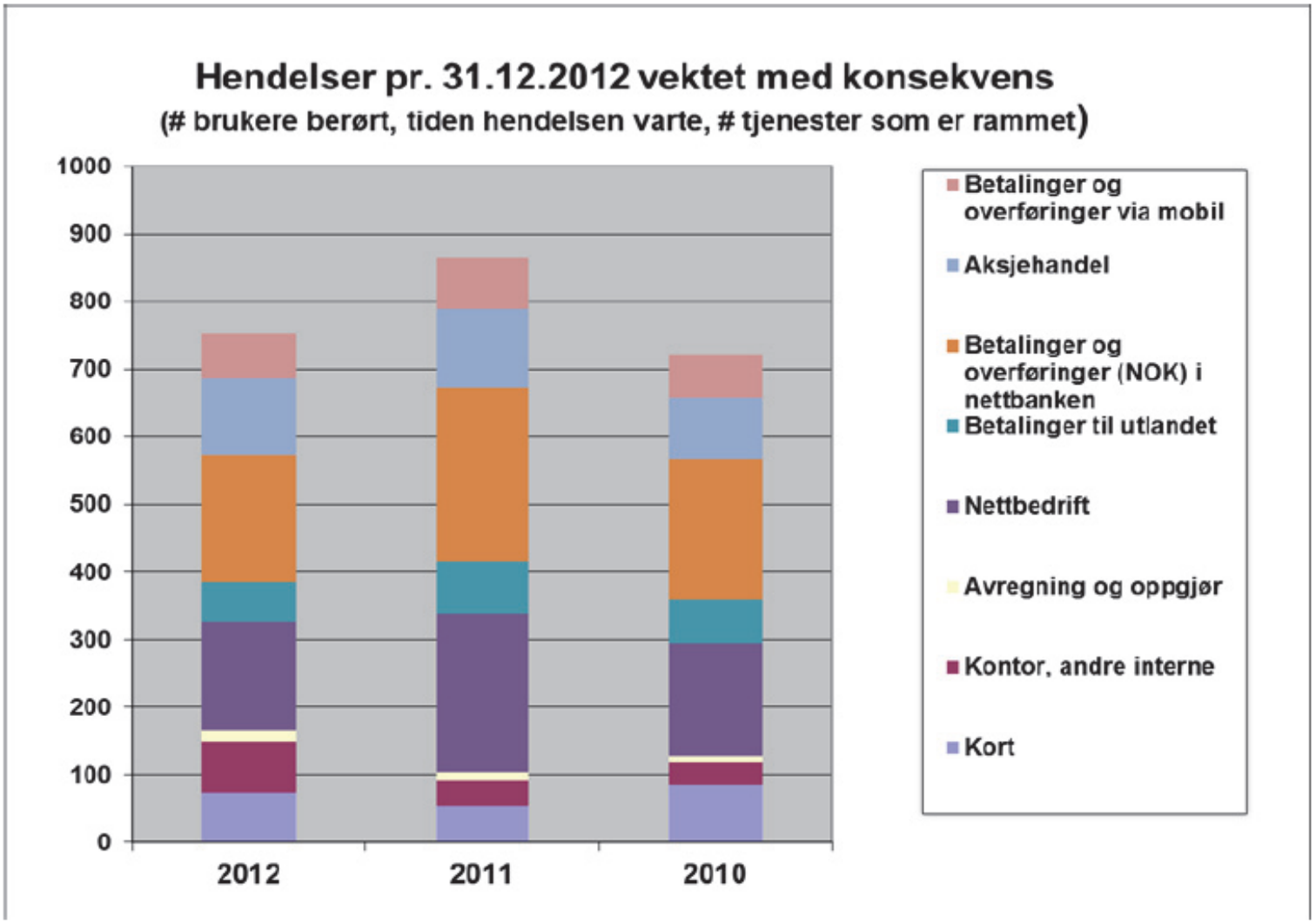
- Mange sentrale løsninger er fra 1980- og 90-årene.
- Modernisering skjer på utsiden.
- Teknologi og kompetanse kan bli vanskelig å opprettholde.
- Å vente for lenge kan representere en risiko – økt kompleks drift.
- Viktig med statusanalyser og klargjøring av problemstillinger.

Tilgang til betalingstjenester

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

- Årlig risikovurdering – identifisere tiltak
- Effektiv håndtering av hendelser – hendelser må benyttes til forbedring
- Identifisere kritiske komponenter
- Sikre nødvendige kontinuitetsløsninger
- Katastrofeløsning og testing – ende-til-ende
- Etablere nødvendig styring og kontroll
- Forstå behovet for monitorering

Figur 8: Hendelser vektet med konsekvens



Finanstilsynets videre oppfølging

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

1. IT-tilsyn og tett kontakt
2. Hendelsesrapportering
3. Arbeid med betalingstjenester
4. Meldeplikt ved endringer og etablering av nye betalingstjenester
5. Beredskapsarbeid

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Cyber Crime

We are building our lives around our wired and wireless networks. The question is, are we ready to work together to defend them?

The FBI certainly is. We lead the national effort to investigate high-tech crimes, including cyber-based terrorism, espionage, computer intrusions, and major cyber fraud. To stay in front of current and emerging trends, we gather and share information and intelligence with public and private sector partners worldwide.

FINANSTILSYNET
THE FINANCIAL SUPERVISORY AUTHORITY OF NORWAY

Takk for oppmerksomheten!

Frank Robert Berg

frb@finanstilsynet.no