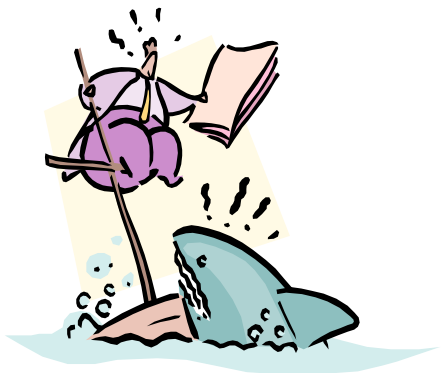
Hvordan å kommunisere sikkerhet innad i virksomheten?



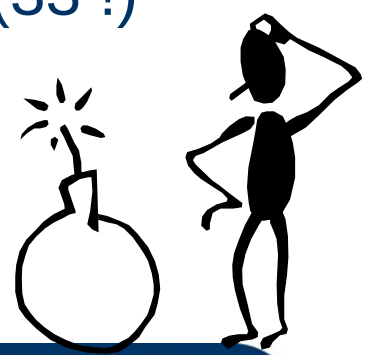
Ove Olsen, SINTEF IKT

Forutsetninger

- I databransjen siden 1973
- IT revisor 1983-1985
- Sikkerhetssjef i EDB Fellesdata 1985-2002
- Daglig leder Senter for informasjonssikring (SIS) 2003-2006
- Medlem av Datakrimutvalget i NSR

Situasjonsbeskrivelse

- Norge er langt framme i verdensmålestokk mht bruk av IT
- Utallige kilder er tilgjengelige for å få kjennskap til IKT trusler
  - Mørketallsundersøkelsen annet hvert år
  - Internett, mailinglister og lignende
  - Offentlige kilder som NorCERT og NORSIS
- Antallet virksomheter som har egen sikkerhetssjef øker stadig
- Krav til sikkerhet i utallige lover og forskrifter (33 !)
- MEN SER VI EN POSITIV BEDRING?



Påstand

- Manglende sikkerhet skyldes ikke mangel på kunnskap om truslene eller manglende hjelpemidler
- Det er heller manglende vilje til å benytte seg av tilgjengelige ressurser

!

Hvem skal vi snakke med?

- Styret
- Toppleder
- Mellomleder
- Medarbeidere
- Konsulenter
- Leverandører
- Besøkende
- Omverden

- Men budskapet må varieres

Manglende praktisering av ansvar

- Styret har overordnet ansvar i hht aksjeloven, men setter sjeldent sikkerhet på agendaen
  - Styret bør minst en gang pr år få rapportert risikostatus IKT
- Administrerende har daglig ansvar, men stoler på sikkerhetssjef når det gjelder sikkerhet
  - Administrerende bør periodisk behandle risiko IKT i ledermøter
  - Mellomledere skal avgi status
- Mellomledere prioriterer det som rapporteres til overordnet
  - Hva om bonus ble påvirket av risikostatus?
- Sikkerhetspolitikk er nedskrevet men ikke synlig i handling
- Frata sikkerhetssjefen ansvaret for sikkerhet!

Manglende involvering av medarbeiderne

- Presenter krav til sikkerhet allerede i ansettelses-prosessen
- Gjennomgå krav like etter ansettelse og krev underskrift på at disse er forstått
- Kommuniser krav relatert til den enkeltes arbeidssituasjon
- Kontroller forståelse
- Premier initiativ
- Bruk medarbeidersamtalen til å avstemme holdninger
- Rapporter periodisk fremskritt til ALLE
- Det er lettere å fordøye små drypp enn en stor flom

Risiko angår alle

- Det er alltid noen som ”visste at dette kom til å skje”
- Inviter alle til å delta i risikoprosessen
- La alle få mulighet til å dokumentere ”sine trusler” – analyser og gi tilbakemelding
- Eierskap gir ansvarsfølelse
- Kommuniser risikobilde – legg vekt på effekt av tiltak

Manglende overvåking

- Alle sikkerhetshendelser må dokumenteres og behandles som forbedringsmulighet
- Beregn kostnader ved hendelser
- Aksepter feiltrinn men ikke overse
- Reager på alvorlige overtramp
- Vurder alltid om forholdet skal meldes til politi

Bevisstgjøring

- Periodisk øvelse gjennom scenarier
- Informer om hendelser hos andre
- Kampanjer
- Konkurranser
- Utmerkelser
- Hvorfor skal bare sikkerhetssjefen reise på kurs?
- Møteplasser/ arenaer
- Jag sikkerhetssjefen ut i organisasjonen!

Oppsummering

- La hele organisasjonen få mulighet til å delta i forbedringen av sikkerheten
- Aksepter at ROM ikke bygges på en dag, og gi ros for de små steg
- Involvering er den beste måten å få medarbeideren til å forstå innholdet i sikkerhetspolitikken
- Vis med handling at dette er viktig

”Det er sannsynlig at noe usannsynlig vil skje”

(Aristoteles)

Men du behøver ikke å sitte uvirksom å vente på dette.

Lykke til !