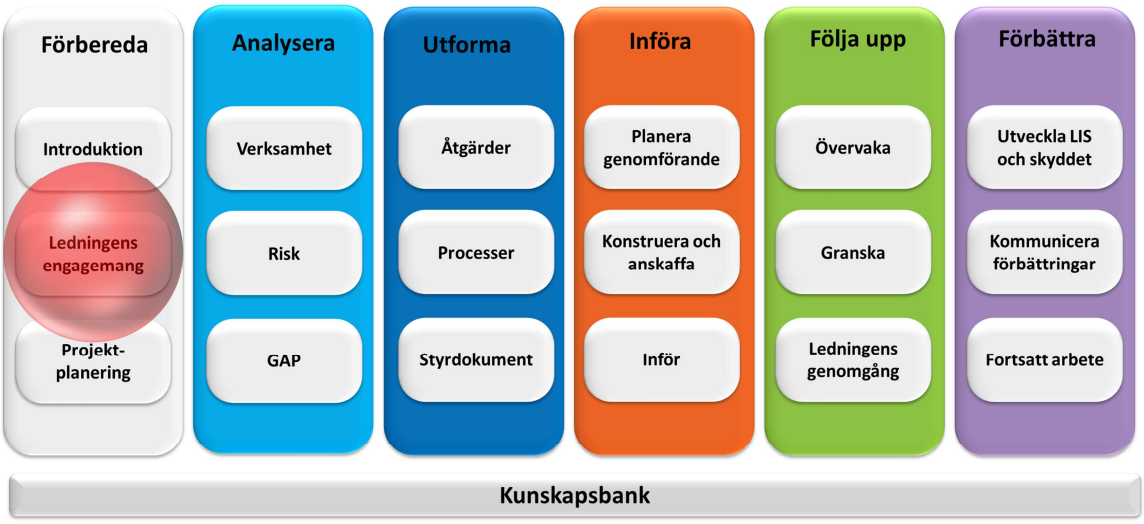
Myndigheten för samhällsskydd och beredskap

Säkra ledningens engagemang



Det här dokumentet är en del av metodstödet som finns att tillgå på www.informationssäkerhet.se

Författare
Helena Andersson, MSB
Jan-Olof Andersson, RPS
Fredrik Björck, MSB konsult (Visente)
Martin Eriksson, MSB
Rebecca Eriksson, RPS
Robert Lundberg, MSB
Michael Patrickson, MSB
Kristina Starkerud, FRA

Publicering
Denna utgåva publicerades 2011-12-15

Innehållsförteckning

1. Inledning

Ledningen har det övergripande ansvaret för informationssäkerheten inom sin organisation och är ytterst ansvarig vid incidenter. En ledning som är engagerad och införstådd med verksamhetsnyttan med informationssäkerhetsarbetet skapar förutsättningar för en hög säkerhetsmedvetenhet i hela organisationen.

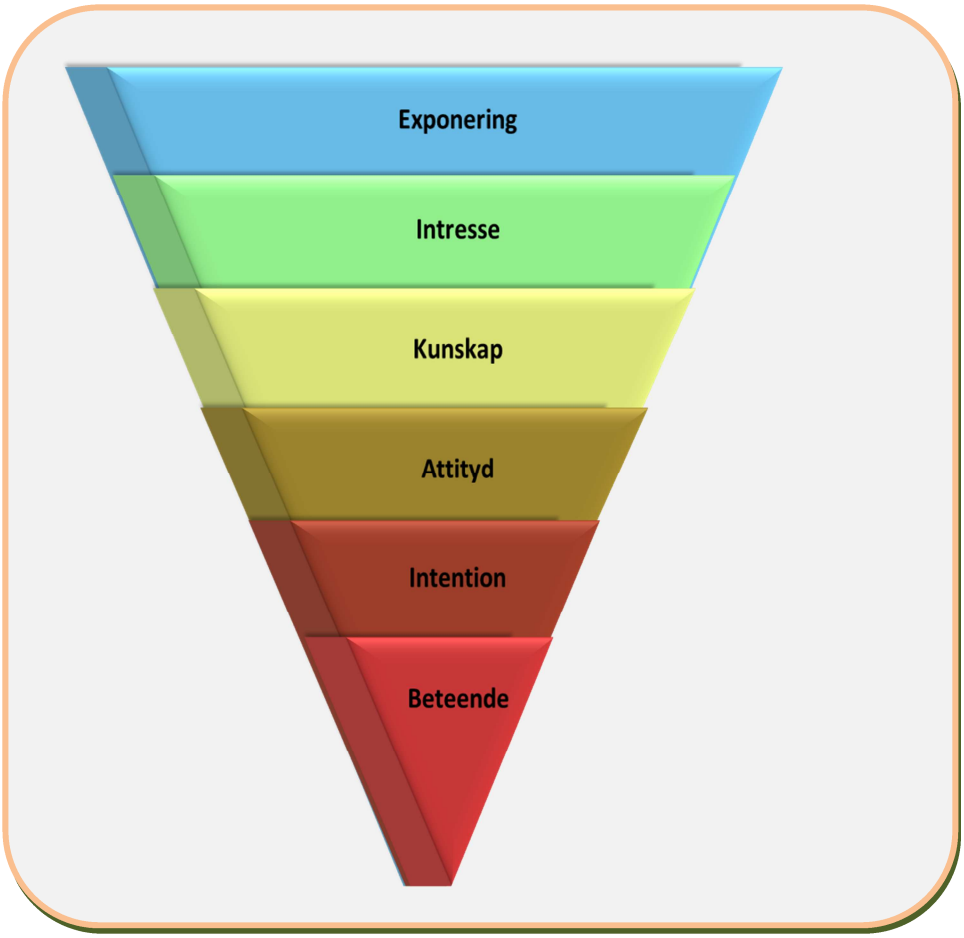
Att få ledningen inom en myndighet, kommun, företag eller annan organisation att förstå vikten av ett strukturerat informationssäkerhetsarbete är viktigt. Detta är de flesta som arbetar med informationssäkerhet medvetna om men många befinner sig i en liknande situation där man har svårt att nå fram till ledningen och få den att förstå att hela organisationen har mycket att vinna på ett väl fungerande informationssäkerhetsarbete.

I denna skrift har vi samlat goda råd och tips till dem som är i början av arbetet med att införa ett ledningssystem och står inför uppgiften att engagera ledningen i arbetet. Materialet har samlats in från informationssäkerhetsexperter med lång erfarenhet ifrån olika typer av organisationer, näringsliv såväl som offentlig förvaltning. Syftet är att materialet ska underlätta för informationssäkerhetssamordnaren att:

- tydliggöra vilken betydelse informationssäkerhet har för verksamheten
- skapa engagemang hos ledningen
- säkerställa att ledningen fattar nödvändiga beslut för att sätta igång arbetet med att införa ett LIS.

På samma sätt som när man kommunicerar ett budskap och vill att det ska resultera i en beteendeförändring i organisationen så måste man även ge ledningen möjlighet att stegvis bygga upp intresse och kunskap för frågan för att det sedan kunna fatta välunderbyggda beslut om informationssäkerhets-arbetet. Nedan pyramid visar utvecklingen från exponering för en fråga till hur det resulterar i en beteendeförändring och, i samband med det, engagemang i frågorna.

Figur 1. Från exponering till beteendeförändring



2. Det första steget

De allra flesta organisationer skyddar sin information på något sätt. Det kan vara genom tekniska hjälpmedel eller mer eller mindre uttalade rekommendationer till personalen, exempelvis skulle få organisationer godta att känslig information publicerades på organisationens webbplats.

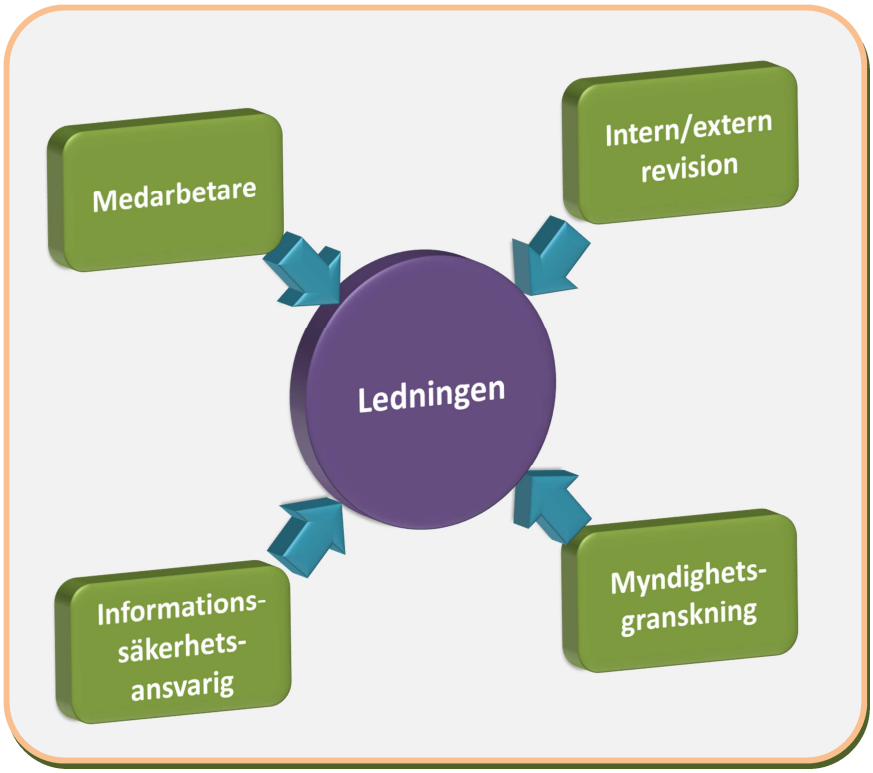
Även om visst säkerhetsarbete redan finns på plats så är det inte säkert att det ger ett heltäckande skydd eller att skyddet är på rätt nivå. En organisation är därför i princip alltid betjänt av att börja arbeta mer systematiskt med informationssäkerhetsfrågorna, exempelvis genom att införa ett LIS eller på annat sätt.

Ledningen har en avgörande roll för informationssäkerhetsarbetet i organisationen, särskilt om arbetet ska ske på ett strukturerat och systematiskt sätt. I vissa organisationer är ledningen redan starkt engagerad medan i andra har informationssäkerhetsfrågorna ännu inte hamnat på ledningens agenda. I de senare fallen är det viktigt att arbeta stegvis för att säkra ledningens engagemang för dessa frågor. Nedan följer en kort redogörelse för vilka budskap och vilka metoder man kan använda för att börja arbetet med att engagera ledningen i informationssäkerhetsarbetet.

2.1 Initiativtagaren

Initiativet till att börja arbeta mer systematiskt och lyfta upp informationssäkerhetsfrågorna kan komma från flera håll. Det kan vara ledningen själv eller den som är ansvarig för informationssäkerheten i organisationen som upplever att brister i informationssäkerhetsarbetet får konsekvenser/kan få konsekvenser. Anledningen till att ett initiativ tas kan exempelvis grundas på att organisationen har råkat ut för en incident eller att medarbetare påtalar att informationssäkerhetsbrister påverkar deras arbete. I figur 2 visas några vanliga initiativvägar.

Figur 2. Vägar för att lyfta informationssäkerhetsfrågor



Oberoende varifrån initiativet kommer behöver den högsta ledningen få ett underlag för att kunna fatta beslut om att gå vidare i informationssäkerhetsfrågan. Många gånger sker det genom att den informationssäkerhetsansvariga gör en första presentation för ledningen.

2.2 Den första presentationen

Den är viktigt att vara väl förberedd första gången man vill lyfta fram och föreslå att organisationen börjar arbeta med informationssäkerhet på ett mer systematiskt sätt. Oftast har man inte så mycket tid till sitt förfogande och det gäller då att lyfta upp rätt budskap för att kunna väcka ledningens intresse för frågan. Målet för den första presentationen är att ledningen ska ge den som är ansvarig för informationssäkerhetsarbetet i organisationen i uppdrag att utreda behovet av vidare arbete.

Vid den första presentationen är det viktigt att lyfta fram frågor som engagerar ledningen och visar på kopplingen mellan verksamhetens behov och informationssäkerhetsarbete. Eftersom det är ytterst få organisationer, om några, som inte på ett eller annat sätt använder information i sin verksamhet finns ofta många kopplingar att lyfta upp. Det mest väsentliga för en ledning är affärsverksamheten, det vill säga uppnå verksamhetens mål. Andra delar är kundnytta, att skydda verksamhetens och sitt eget varumärke, undvika negativ publicitet, upprätthålla kontinuiteten, hur man kan undvika informationsläckage.

När man vill lyfta upp betydelsen av informationssäkerhet är det lätt att hamna i en situation där man endast fokuserar på riskerna med bristande informationssäkerhet och går in i tekniska resonemang. Detta kan få ledningen

att börja se på informationen som skrämselpropaganda och att det är en ren teknisk fråga. Händer detta är det svårare att väcka tillräckligt mycket intresse hos ledningen för att de ska vilja engagera sig i det fortsatta arbetet.

Betona gärna istället nyttan med att arbeta systematiskt och långsiktigt med informationssäkerhet. Här kan man använda en faktisk incident som exempel och visa på positiva effekter, exempelvis som viktigt bidrag till verksamhetens effektivitet. Det är bra att lyfta fram vikten av att man kan säkerställa att information som inte får spridas till obehöriga ges ett fullgott skydd och att information som behövs i verksamheten vid en viss tidpunkt då verkligen finns till medarbetarnas förfogande. Använd gärna metaforer från den fysiska världen.

Det går att förbereda sig på flera sätt men generellt kan sägas att det är bra att ta fram följande underlag inför en första presentation:

- en gapanalys där man översiktligt har analyserat nuläget i förhållande till de förslagna säkerhetsåtgärderna i 27002
- informationssäkerhetsincidenter som drabbat organisationen senaste tiden
- de senaste IT- revisionsrapporterna
- vilka fördelar för ledningen som ett systematiskt informationssäkerhetsarbete kan ge, exempelvis tillgång till tekniska hjälpmedel som underlättar deras arbete.

2.3 Vilket budskap bör lyftas fram?

Det är viktigt att känna till kulturen i sin organisation, vissa har en kultur av regelstyrning och andra av riskstyrning. Försök anpassa till organisationens kultur. Under den första korta presentationen för ledningen bör både positiva effekter med ett gott informationssäkerhetsarbete lyftas fram samt konsekvenserna av brister i informationssäkerhetsarbetet. De positiva delarna med ett systematiskt informationssäkerhetsarbete bör framhållas framför konsekvenserna vid bristande säkerhetsarbete. Det är bra om ledningen förknippar informationssäkerhet med något positivt och att det inte är så komplicerat. Denna positiva inställning kan de sedan kommunicera ut i organisationen.

Alla organisationer råkar förr eller senare ut för incidenter vilka kan få negativa konsekvenser för verksamheten, exempelvis i form av ekonomiska förluster. Det kan vara positivt att lyfta upp hur konsekvenserna av incidenter kan begränsas genom att ha kunskap om vilken information som behöver skyddas och vilket skydd som krävs. Andra faktorer som begränsar konsekvenserna och som är viktigt att presentera är utbildning av all personal i informationssäkerhet och att arbeta systematiskt och organiserat med sin informationssäkerhet. Andra budskap kan vara att:

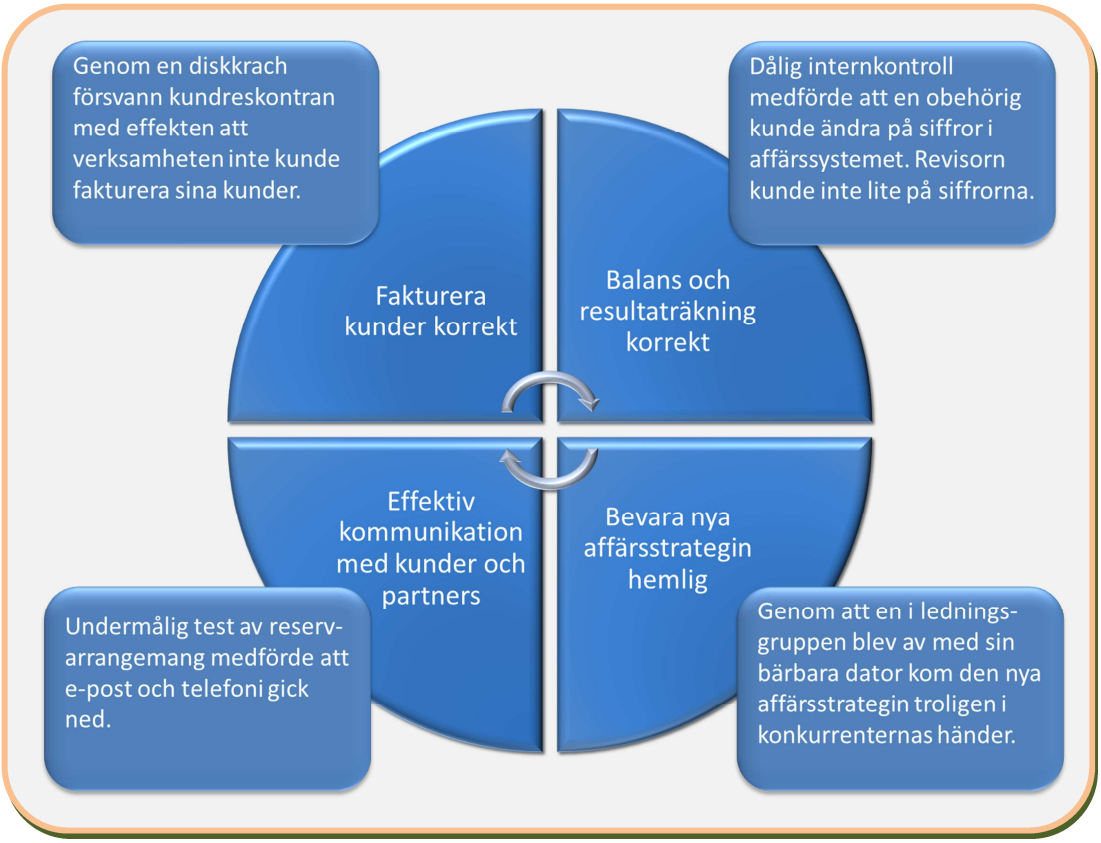
- Genom att medarbetarna har tillgång till rätt information vid rätt tidpunkt kan effektiviteten ofta höjas.
- Med ett strukturerat informationssäkerhetsarbete går det att förhindra att information avslöjas till obehöriga, till exempel för en konkurrerande verksamhet. Ett sådant avslöjande kan, beroende på vad det är för information, leda till att konkurrenterna kan försöka ta över kunder, motarbeta affärsstrategin och kanske till och med bidra till att svärta verksamhetens rykte på marknaden.

Att ge exempel från vad liknande verksamheter har råkat ut för på grund av brister i informationssäkerhetsarbetet ger ofta lättare förståelse för frågorna. Exempel som kan relateras till följande punkter är ofta av intresse eftersom ledningen inte vill:

- få negativ publicitet
- förlora affärer (pengar)
- få informationsläckage
- få driftstopp

Figur 3 visar på sambanden mellan ovan punkter och olika processer i organisationen.

Figur 3. Samband mellan incidenter och processer



2.4 Metod

Ta fram en bild som beskriver flödet. Det finns naturligtvis många sätt att kort väcka ledningens intresse för informationssäkerhetsfrågorna. Olika organisationer har även olika fokus. Ett företag och en myndighet regleras delvis av olika rättsliga regelverk och kan därför betrakta olika risker som särskilt allvarliga. Som exempel på några utgångspunkter för den första presentationen som passar de flesta organisationer kan nämnas:

- Anknyt till verksamheten och använd exempel som ligger nära den egna verksamheten Det är lättare för en person i ledningen att förstå frågorna om man kan visa på exempel på incidenter som faktiskt hänt inom den egna organisationen och exempel från närliggande verksamhet.
- Undvik teknisk terminologi.
- Låt ledningsgruppen själva göra en enkel uppskattning av risker och konsekvenser, gärna ekonomiska och rättsliga, av exempelvis förlust av viss känslig verksamhetsinformation beroende på organisation kan man ta det på olika nivåer. Exempelvis kan en enklare workshop göras.

- Titta på vilken kompetens som finns hos den som redovisar detta för ledningen. Ibland kan det vara bra att lämna över det till en annan person. De måste känna att det är vi som äger frågan. Förankra det eventuellt hos någon i ledningen innan. Vem är det som sponsrar dig som informationssäkerhetsansvarig?

- Förklara och betona betydelsen av ledningens engagemang i arbetet samt att de är ytterst ansvariga för att information hanteras säkert i organisationen.

- Ge ett konkret förslag på nästa steg, företrädesvis att påbörja arbetet genom att den som är ansvarig för informationssäkerhetsarbetet ska återkomma med ett förslag på hur man bör gå vidare.

    1. Om ledningen är mogen att påbörja arbetet i det här skedet – föreslå att ett projektdirektiv tas fram och redovisas för ledningen

    2. Om det fortfarande finns tveksamheter hos ledningen för behovet av satsningen (vi har redan en bra informationssäkerhet) - föreslå att en grundlig gapanalys genomförs och att resultatet redovisas för ledningen

Efter den första presentationen följer arbetet med att förbereda underlag för de beslut som ledningen behöver ta för att arbetet med att införa ett ledningssystem för informationssäkerhet kan påbörjas.

3. Beslut om införande

Här är det viktigt att tänka på verksamhetsplaneringscykeln. Timingen är central när man lyfter upp frågan om att införa ett LIS Det kan vara bättre att ta upp frågan om införande i god tid inför nästa års verksamhetsplanering istället för att hasta och försöka få ett beslut innevarande år. Förankringsarbetet tar tid och bör påbörjas i god tid. För att projektet ska kunna genomföras på ett effektivt sätt räcker det dock inte med ett generellt hållet beslut om att starta ett sådant projekt. Det är lika viktigt att ledningen klargör ansvar, roller och tillser att resurser finns. De måste även känna engagemang för arbetet och se till att det kommuniceras ut i organisationen. Återanvänd det som redan finns i form av exempelvis policy, gjorda informationssäkerhetsanalyser etcetera.

3.1 Vilka beslut behöver ledningen fatta

När ledningen har engagerats och kommit fram till att verksamheten ska uppfylla kraven i 27001 är ytterst viktigt att ledningen formellt beslutar om att införa ett LIS. Beslutet bör bygga på att ledningen är engagerad och förstår vilken nytta verksamheten har av informationssäkerhetsarbetet. Det är viktigt att den som är ansvarig för informationssäkerheten ser till att ledningen får ett bra beslutsunderlag. Stöd kan bland annat hittas i dokumentet ”Projektplanering”. Följande beslut behöver ledningen fatta:

- **Den högsta ledningen ska fatta beslut om att införa ett ledningssystem för informationssäkerhet i sin verksamhet.** Beslutsdokumentet kan peka på att verksamheten ska uppfylla kraven i standarden SS-ISO/IEC-27001, Ledningssystem för informationssäkerhet och att arbetet ska bedrivas i enlighet med standarden SS-ISO/IEC-27002, Riktlinjer för styrning av informationssäkerhet. Ledningen bör även här sätta ambitionsnivån för LIS-arbetet. Det är viktigt att den nivån inte sätts för högt då risken finns att projektet fastnar i ett tidigt skede och inte kommer vidare.

  Alla organisationer har ett ledningssystem, eller ett ”system” för ledning av verksamheten. Det handlar helt enkelt om hur ledningen styr verksamheten. Ett ledningssystem för informationssäkerhet är därmed den del av ledningssystemet som styr informationssäkerheten i verksamheten. En viktig del av ledningssystemet är de interna styrande dokument som reglerar informationssäkerhetsområdet. Dessa dokument bör följa den struktur som organisationen har för styrande dokument på andra områden. I det här stadiet är det även viktigt att förklara relationen mellan LIS och andra ledningssystem, exempelvis för miljö eller kvalitet.

- **Den högsta ledningen bör utse någon som får samordningsansvar för organisationens informations-säkerhet.**
  Denna bör vara placerad i organisationsstrukturen på ett sådant sätt att det ger ett tydligt mandat och en löpande rapporteringsmöjlighet direkt till verksamhetens högsta ledning. Det är inte lämpligt att den som ansvarar för informationssäkerhet placeras på IT-avdelningen. Den samordningsansvariga bör ha tillräcklig kompetens inom området och erfarenhet från att driva projekt.

- **Den högsta ledningen bör se till att det finns en strategi för kommunikation ut i den egna organisationen rörande LIS-arbetet.**
  Viktigt att alla i organisationen får information från ledningen om att detta arbete sker. Sedan bör kontinuerlig information förmedlas ut i verksamheten, t ex. när den övergripande informationssäkerhetspolicyn är beslutat av ledningen. I sin kommunikationen är det också viktigt att ledningen ger tydliga signaler ut i verksamheten om att den informationssäkerhets¬ansvariga har en viktig uppgift och får tydliga mandat. Beskriv vilka effekter och/eller konsekvenser (positiva, negativa, neutrala) ett genomförande av LIS-arbetet skulle innebära för verksamheten.

- **Den högsta ledningen bör fatta beslut om budget för LIS-arbetet både när det gäller ekonomiska ramar och personalresurser samt arbetstimmar.**
  För att ledningen ska kunna avsätta resurser för ett sådant arbete bör den få ett så bra underlag som möjligt. Kostnaderna för att införa ett LIS kan mätas i de resurser och den tid som avsätts för arbetet samt i investeringskostnaderna för olika säkerhetsåtgärder. Däremot är det svårare att beräkna kostnaden för att inte vidta några informationssäkerhetsåtgärder. En riskanalys är det bästa sättet att skaffa sig en uppfattning om kostnaden för säkerhets¬investeringarna samt om den alternativa kostnad som bristen på sådana investeringar kan medföra. I riskanalysen analyseras sannolikheten för att ett hot ska realiseras och vad som händer om hotet blir verklighet – både ekonomiska och andra konsekvenser. Detta måste sedan ställas mot kostnaden för skyddet och alternativkostnaden i form av vad man i stället kunde använda pengarna till. Redan inträffade incidenter kan självfallet användas som underlag för att beräkna om en säkerhetsinvestering lönar sig eller inte.

3.2 Argument för att införa ett LIS i organisationen

Det finns ett antal argument som kan användas för att få ledningen engagerad i ett LIS-arbete eller integrerat LIS:

- Med ett LIS är det lättare att uppfylla de legala krav på informationssäkerhet som finns, exempelvis i personuppgiftslagen (1998:204) och i MSB:s föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2009:10).
- Ett LIS ger även organisationen bättre möjligheter att arbeta på ett modernt sätt. Exempelvis strävar många myndigheter att utnyttja teknikens möjligheter och bli en ”e-myndighet”.
- Med rätt säkerhetsnivå kan verksamheten bedrivas i enlighet med verksamhetsmålen.
- Verksamheten får en god informationssäkerhet som är anpassad efter de aktuella förutsättningarna och behoven.
- Ledningen får genom LIS ett verktyg för att följa och kontrollera informationssäkerheten.
- Verksamheten får riktlinjer och instruktioner som gör det lättare att bevara och höja säkerheten.
- Det blir tydligt för alla vem som har ansvaret för informationssäkerhet.
- Säkerhetsmedvetandet ökar i hela organisationen.
- Det blir lättare att identifiera och åtgärda viktiga brister.
- Omvärlden ser att verksamheten lägger stor vikt på kvalitet och säkerhet i informationshanteringen, vilket krävs för att få intressenternas fortsatta förtroende.
- Då allt fler företag och organisationer följer internationella standarder på området och certifierar sig mot den (SS-ISO/IEC 27001) blir det ett allt viktigare verktyg för att skapa konkurrensfördelar.
- Vilka pengar har lagts ner i sin it-miljö. Fråga ledningen. Visa på tillgångens värde. Så här mycket pengar har vi investerat här men då har vi inte sett värdet av informationstillgången, system etc.

4. Kontinuitet för ledningens engagemang

För att LIS-projektet inte ska stanna upp är det viktigt att ledningen kontinuerligt följer arbetet. Den person med utpekat samordningsansvar bör löpande få möjlighet att redovisa hur arbetet fortskrider för ledningen. Ledningen bör också aktivt stödja arbetet med informationssäkerhet genom att föra upp frågorna på agendan i olika sammanhang, se till att projektet har tillräckligt med resurser samt ge ansvar och befogenheter till de berörda parterna. De beslut som ledningen fattar under projektet gång bör spridas i organisationen i syfte att förankra intentionerna. Ledningens genomgång beskrivs i delprocessen ”Följa upp”.