

LÖNSAM SÄKERHET

METODBOK



Klas Nilsson

Lönsam säkerhet

Metodbok

av

Klas Nilsson, CPP, PCI, PSP, CFE, CISM

Upphovsrättsinnehavare 2026 © Klas Nilsson

Mångfaldigande av innehållet i denna bok, helt eller delvis, är enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk förbjudet utan medgivande från författaren. Förbudet gäller tryckning, kopiering, skanning, bandinspelning med mera samt lagring på datamedia.



www.securitymanager.se
info@securitymanager.se

Författare: Klas Nilsson
Redigering: Klas Nilsson
Omslag: Klas Nilsson
Vissa bilder är AI-genererade,
andra är köpta från Shutterstock
ISBN: 978-91-531-8766-0

Innehållsförteckning

Prolog	7
Om författaren	9
Introduktion	13
Säkerhetsrelaterade kostnader	14
Skyddskostnad och skadekostnad	14
Säkerhetsrelaterade intäkter	15
Överdrivna skyddsåtgärder	16
Kompensatoriska skyddsåtgärder	18
Optimala skyddsåtgärder	19
Sambanden mellan centrala områden	20
Modellen för lönsam säkerhet	24
Bokserien Lönsam säkerhet	25
Tillgångar	29
Varför tillgångar är utgångspunkten för lönsam säkerhet	29
Metodisk arbetsordning	30
Att sätta ett monetärt värde på tillgångar	36
Befintliga skyddsåtgärder	37
Hotbild	41
Hotbild är inte en lista på hot	41
Nulägesbild – hur hot har manifesterats hittills	42
Från beskrivande till prediktiv analys	48
Incidentrapportering och budgetering av skadekostnader	50
Konsekvens	55
Konsekvens – från hot till skadekostnad	55
Konsekvens och återhämtningsförmåga	60
Metod	73
Tillgångar och deras egenskaper	74
Överväganden vid val av metod	77
Organisation	87
Organisation i en föränderlig omvärld	88
Organisationens tre ingångsvärden	90
Ledarstilar och deras betydelse för säkerhetsarbetet	93
Förmågutveckling – från plan till resultat	95
Organisationens mognad och säkerhetskultur	97
Kriskommunikation som organisatorisk förmåga	99
Effektivitet	105
Funktion eller prestation	106
Principer för ett effektivt skydd	108
Principer för effektiv kontinuitet	111
Investering	119
Två grundläggande kostnadstyper	120
Att räkna – utan att fastna i matematik	122

Lönsamhet	129
Vad menas med lönsamhet i säkerhetsarbete?	129
Skyddskostnaden – vad kostar säkerhet egentligen?	131
Optimal säkerhet – inte maximal	137
Mätetal	143
Varför mätetal behövs i säkerhetsarbete	143
Lönsam säkerhet i accelerationen	159
När tid blir affärens hårdvaluta	159
Beslutsnivå – när säkerhet blir styrning, inte teknik	161
Riskacceptans – när att avstå blir en strategisk kompetens	162
Förändringstakt – när världen går i flera tempon samtidigt	163
Ordlista	169
Modellens tillämpningsområde	189
Register	192
Epilog	197
Bokserien Lönsam säkerhet	198

Om du kunde, skulle du välja bort säkerhetsarbetet?

Prolog

Alla verksamheter har säkerhetsrelaterade kostnader. Antingen betalar man för skydd i form av personal, lås, larm och arbetstid eller så betalar man för bristande skydd genom skador, avbrott, sanktionsavgifter och förluster. Det är fullt möjligt att uppfylla fastställda krav och till och med optimera enskilda skyddsåtgärder och ändå ha höga säkerhetsrelaterade kostnader. Först när säkerhetsarbetet utgår från verksamhetens risker och affärsmål blir det möjligt att styra mot en bättre totalekonomi, där skyddskostnaden faktiskt minskar skadekostnaden mer än den själv kostar.

När jag började arbeta med säkerhet i början av 1990-talet handlade det mest om att uppfylla försäkringskrav och branschkrav. Säkerhet sågs då som en nödvändig särkostnad, något som behövde finnas för att kunna göra affärer, men som inte förväntades skapa värde. Sedan förändrades förutsättningarna. Ny teknik skruvade upp utvecklingstakten och nya hotbilder gjorde konsekvenserna både större och mer komplexa. Det som tidigare kunde hanteras med fasta krav och etablerade lösningar började kräva ett annat sätt att tänka.

Det var år 2003, när jag började studera för personcertifieringen CPP, som jag fick upp ögonen för något avgörande: säkerhet kan, i mycket större utsträckning, utformas utifrån riskanalyser och ekonomisk hållbarhet. Det ledde till att jag började utveckla en metod för att göra säkerhetsarbetet mer styrbart och mer affärsnära. Den största utmaningen har inte varit att skapa lönsamhet i säkerhetsarbetet, utan att övertyga ledningen om att det är möjligt.

Åren 2010–2012 skrev jag Säkerhetsboken 2.0 och året efter Säkerhetsboken 3.0. Då kom delar av resonemanget på pränt. År 2013 tog modellen för lönsam säkerhet sin form, ungefär som den ser ut i skrivande stund och jag började skriva den här boken. Manusets har fått växa fram långsamt, parallellt med praktik och erfarenhet, där verkliga händelser har tvingat fram precision i både begrepp och samband. Resultatet är den här boken, nästan fjorton år senare.

Lönsam säkerhet är ingen motsättning. Det är ett medvetet val.

Turn Security from Cost to Asset

Om författaren

Klas Nilsson har arbetat med säkerhet sedan början av 1990-talet och har mer än trettio års erfarenhet av säkerhetsarbete inom privat och offentlig verksamhet. Under åren har han arbetat som säkerhetschef, säkerhetsskyddschef, konsult, utredare, utbildare och författare inom ett stort antal delar av säkerhetsområdet.

Hans erfarenhet omfattar bland annat säkerhetsledning, fysisk säkerhet, informationssäkerhet, personalsäkerhet, personskydd, säkerhetsskydd, riskhantering, kontinuitet, krishantering och utredningar. Han har arbetat med säkerhetsfrågor inom bland annat finansiell verksamhet, hotell- och besöksnäring, spelverksamhet, IT och telekom, säkerhetsbranschen och samhällsviktig verksamhet.

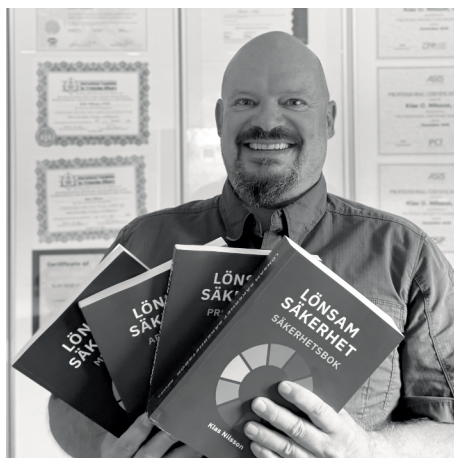
Denna bredd har gett honom erfarenhet av säkerhetsarbete på flera nivåer, från praktiska skyddsåtgärder och utredningar till riskhantering, ledningssystem, verksamhetsutveckling och beslutsunderlag för ledning och styrelse.

Klas Nilsson började utveckla modellen **Lönsam säkerhet** under 2000-talet. Modellen växte fram ur erfarenheten att säkerhetsfrågor ofta beskrivs i termer av hot, risker och krav medan verksamhetens ledning behöver fatta beslut om mål, investeringar, kostnader, prioriteringar och förväntade resultat. Modellen förenar dessa perspektiv och gör säkerhetsarbetet till en integrerad del av verksamhetens styrning och värdeskapande.

Hans syn på säkerhet är pragmatisk, riskbaserad och affärsdriven. Utgångspunkten är att skydda det som verkligen är skyddsvärt och verksamhetskritiskt och välja åtgärder som ger störst nytta för verksamheten. Målet är ett effektivt och lönsamt säkerhetsarbete som bidrar till verksamhetens förmåga att nå och överträffa sina mål.

Klas har studerat kriminologi vid Stockholms universitet och riskhantering i lokalsamhället vid Karlstads universitet samt ekonomi och juridik. Han har vidareutbildat sig inom bland annat informationssäkerhet, projektledning och kriskommunikation.

Han innehar de internationella personcertifieringarna Certified Protection Professional (CPP), Physical Security Professional (PSP), Professional Certified Investigator (PCI), Certified Information Security Manager (CISM) och Certified Fraud Examiner (CFE). Klas Nilsson är författare till flera fackböcker om säkerhet och upphovsman till modellen och bokserien Lönsam säkerhet.





Är säkerhet en kostnad –
eller en dold tillgång?

Introduktion

Säkerhet kostar pengar. Det är allmänt känt. Det som däremot fortfarande är oklart i många verksamheter är vad säkerhetsarbetet faktiskt kan bidra med.

I många styrelserum betraktas säkerhet fortfarande som ett nödvändigt ont. En kostnad som måste bäras för att uppfylla lagkrav, försäkringsvillkor eller för att undvika rubriker i media. Säkerhetsbudgeten ses som en försäkringspremie som man hoppas slippa använda, men som ändå måste betalas. När tiderna blir tuffare är säkerhet därför ofta ett av de områden som ifrågasätts, reduceras eller skjuts på framtiden.

Samtidigt lever vi i en tid där hotbilden är mer komplex, mer föränderlig och mer verksamhetskritisk än någonsin tidigare.

- Cyberangrepp kan slå ut hela verksamheter över en natt.
- Leverantörsstörningar kan stoppa produktion i flera led.
- Informationsläckor kan radera förtroende som tagit decennier att bygga upp.

Ett enda allvarligt avbrott kan få konsekvenser långt bortom den direkta skadan, i form av uteblivna intäkter, skadade relationer, juridiska påföljder och långvarig osäkerhet i organisationen.

Trots detta saknas det ofta ett gemensamt språk mellan säkerhetsfunktionen och verksamhetsledningen. Säkerhet talar risker, hot och sårbarheter. Ledningen talar lönsamhet, tillväxt, effektivitet och affärsmål. När dessa perspektiv inte möts uppstår ett glapp. I det glappet förlorar säkerhetsarbetet både genomslag och legitimitet. Det är detta glapp som den här boken syftar till att minska.

Tänk om säkerhetsarbetet inte bara sågs som en kostnad, utan som ett medel för att skydda intäkter, minska totala kostnader och skapa förutsättningar för affärer som annars inte hade varit möjliga.

Det är här begreppet **lönsam säkerhet** tar sin utgångspunkt.

Lönsam säkerhet handlar inte om att maximera skydd eller minimera kostnader, utan om att optimera sambandet mellan verksamhetens tillgångar, hotbild, konsekvenser och valda åtgärder. Det handlar om att vidta rätt åtgärd, vid rätt tidpunkt, på rätt nivå och att kunna visa vilken effekt det faktiskt ger.

För att lyckas med detta krävs ett annat sätt att tänka kring säkerhet. Ett sätt som kopplar säkerhetsarbete till organisation, investeringar, effektivitet och i slutänden lönsamhet. Det är denna helhetssyn som introduceras i detta kapitel och som resten av boken steg för steg fördjupar.

Säkerhetsrelaterade kostnader

Alla verksamheter har säkerhetsrelaterade kostnader, det vill säga kostnader kopplade till säkerhet, oavsett vilka åtgärder som vidtas eller inte. Det är viktigt att förstå att detta inkluderar både kostnader för att skapa god säkerhet och konsekvenserna av säkerhetsbrister, snarare än bara direkta kostnader för skyddsåtgärder.

En bra jämförelse är personalrelaterade kostnader, som uppstår i flera steg: vid rekrytering (exempelvis rekryteringsprocesser och introduktionsutbildningar), under anställning (lön, utbildningar, administration) och vid avslut (förlorade intäkter, nyrekrytering). På samma sätt kan säkerhetsrelaterade kostnader delas upp i olika kategorier och kontexter, inklusive ineffektiva eller överdimensionerade skyddsåtgärder samt konsekvenser av uteblivet skydd.

Verksamheten kan även ha skyddsåtgärder som inte är ändamålsenliga. Det vill säga inte verksamma mot hotbilden på grund av att de är feldimensionerade, exempelvis för svaga och skadan inträffar i alla fall eller för kraftiga och kostar onödigt mycket eller helt felaktiga för den aktuella hotbilden. Likaså kan det finnas skyddsåtgärder som inte längre behövs på grund av förändrade omvärldsfaktorer eller verksamhetsförändringar. Skyddsåtgärder kan föråldras av slitage, bristande underhåll eller andra omständigheter som gör att de inte längre är effektiva.

Skyddskostnad och skadekostnad

För att uppnå lönsamhet i säkerhetsarbetet behöver man förstå vad som påverkar kostnaderna. Dessa kan delas in i tre huvudkategorier:

- **Skyddskostnad:** Utgifter för åtgärder som förbättrar säkerheten, beroende av valda lösningar och organisationens effektivitet.
- **Skadekostnad:** Kostnader som uppstår när tillgångar skadas på grund av säkerhetsbrister – dvs. avsaknad av lämpligt skydd.
- **Juridiska påföljder:** Sanktionsavgifter, viten, böter och skadestånd vid bristande regelefterlevnad – betraktas här som en typ av skadekostnad.

Reaktivt säkerhetsarbete, dvs. att man agerar först efter en incident, gör att kostnaderna kan skena iväg jämfört med proaktivt arbete. Reaktivitet leder ofta till:

- **Svårare skada**, på grund av avsaknad av tillräckliga skyddsåtgärder.
- **Akuta och dyrare insatser** ofta med extern hjälp.
- **Driftstopp** och förlorade intäkter.
- **Förtroendeförlust** och förlorade kunder.

Säkerhetsrelaterade intäkter

Säkerhetsarbete kan också vara en stark värdeskapare. Genom att arbeta strukturerat med skydd, riskhantering och säkerhetskultur kan verksamheter skapa intäkter, affärsfördelar och stärkt konkurrenskraft. Här är några exempel på hur säkerhet kan bidra till ökad lönsamhet:

- **Nya affärsmöjligheter:** Säkerhetscertifieringar, regelefterlevnad och strukturerat riskarbete gör det lättare att vinna affärer, särskilt hos kunder som ställer krav på informationssäkerhet, kontinuitet eller fysisk säkerhet. ISO 22301, ISO 27001, ISO 28000 och SSF 1101 är exempel på sådant som ökar tilliten.
- **Nya marknader:** Organisationer med god riskhanteringsförmåga kan göra säkrare affärer på osäkra marknader, geografiskt eller branschmässigt, vilket möjliggör affärer där andra aktörer tvekar.
- **Bättre beslutsunderlag:** Säkerhet handlar om att undanröja risk och skapa visshet. Riskanalyser, händelsedata och strukturerade rutiner ger ledningen bättre information för att styra verksamheten framåt, med färre överraskningar och bättre precision.
- **Operativ effektivitet:** Säkerhet skapar ordning och tydlighet i processer, rutiner, instruktioner och tekniska lösningar, vilket minskar fel, avbrott och ineffektivitet. Det höjer produktiviteten och främjar ett mer proaktivt arbete.
- **God säkerhetskultur:** En trygg och välorganiserad arbetsmiljö stärker medarbetares engagemang, lojalitet och stolthet. Det gör det lättare att behålla och attrahera kompetens, vilket i sin tur stärker verksamhetens långsiktiga stabilitet.
- **Sänkta försäkringskostnader:** Ett dokumenterat säkerhetsarbete sänker riskprofilen, vilket kan ge lägre premier, självrisker och bättre försäkringsvillkor. Detta innebär en direkt ekonomisk besparing.
- **Färre kostsamma incidenter:** Förebyggande säkerhet minskar risken för driftstopp, dataintrång, juridiska sanktioner och skadestånd. Att inget oönskat händer till följd av fungerande skydd är ett affärsvärde i sig.
- **Differentiering och kvalitetsintryck:** Ett väl fungerande säkerhetsarbete är också en symbol för kvalitet, ansvar och professionalism. Det kan användas i marknadsföring, anbud och kommunikation för att stärka varumärket.

Ett genomtänkt säkerhetsarbete bidrar till ökade intäkter, minskade kostnader, ökad stabilitet och bättre beslutsfattande. Det är inte en kostnadspost utan en investering i förtroende, effektivitet och affärsutveckling.

Överdrivna skyddsåtgärder

Överdrivna skyddsåtgärder kännetecknas av att skyddskostnaderna är höga samtidigt som den faktiska minskningen av skadekostnaderna är liten eller obefintlig. I dessa fall har säkerhetsarbetet passerat den punkt där ytterligare skydd ger proportionerlig nytta. Skyddet kan upplevas som omfattande och robust, men leder i praktiken till ökande totalkostnader och försämrad lönsamhet.

Till skillnad från kompensatoriska skyddsåtgärder, där skyddskostnader och skadekostnader tar ut varandra så att totalkostnaden förblir oförändrad, innebär överdrivna skyddsåtgärder att skyddskostnaderna ökar snabbare än skadekostnaderna minskar. Säkerhetsarbetet blir därmed direkt kostnadsdrivande.

Ett vanligt sätt som överdrivet skydd uppstår på är genom felriktade skyddsåtgärder. Organisationen investerar i avancerade, tekniskt sofistikerade eller kostsamma lösningar utan tydlig koppling till den faktiska hotbilden. Skyddet dimensioneras för scenarier med låg sannolikhet eller begränsad konsekvens, medan mer sannolika och vardagliga risker inte adresseras i motsvarande utsträckning. Resultatet blir höga investerings- och driftskostnader med begränsad effekt på de skador som faktiskt inträffar.

Överdrivet skydd uppstår också ofta när verksamheten förändras över tid, men skyddsnivåerna inte omprövas. Skydd som en gång var rationellt i en riskfylld miljö kan bli kvar trots att hotbilden minskat eller förändrats. Ett exempel är verksamheter som tidigare haft särskilt skyddsvärd produktion eller funktion, men som senare ändrat inriktning. Om kostsamma tekniska skydd, bevakning och administrativa krav behålls oförändrade, uppstår ett permanent överdimensionerat skydd som inte längre står i proportion till den aktuella risken.

Ett närliggande exempel är överdriven säkerhetsklassning av personal. I verksamheter med höga säkerhetskrav kan många befattningar initialt placeras i säkerhetsklass, vilket är fullt motiverat utifrån den dåvarande hotbilden och verksamhetens inriktning. När roller, arbetsuppgifter eller verksamhetens förutsättningar senare förändras kan behovet av säkerhetsklassning i vissa delar av organisationen minska, medan det i andra delar kan kvarstå eller till och med öka.

Problemet uppstår när organisationen inte omprövar vilka befattningar som faktiskt behöver vara säkerhetsklassade i relation till den aktuella hotbilden. Om antalet säkerhetsprövade personer då förblir oförändrat trots att behovet minskat i delar av verksamheten, kvarstår kostnaderna för säkerhetsprovningsintervjuer, utbildningar och administrativ hantering utan motsvarande säkerhetsnytta. Resultatet blir ett personellt skydd som är överdimensionerat i förhållande till den faktiska risken och därmed kostnadsdrivande.

Överdrivna skyddsåtgärder uppstår även när skyddet inte tar hänsyn till mänskligt beteende. Ett vanligt exempel är mycket strikta och komplexa lösenordskrav. I syfte att höja säkerheten införs långa och svårhanterliga lösenord, vilket i praktiken leder till att medarbetare skriver ner dem på lappar, sparar dem oskyddat eller återanvänder dem på olämpliga sätt. Skyddsåtgärden blir dyr att administrera, genererar fler supportärenden och skapar nya sårbarheter, samtidigt som den faktiska säkerheten inte förbättras. I många fall hade enklare lösningar, kombinerade med tekniska begränsningar som spärrar efter upprepade felaktiga inloggningar, gett bättre skydd till lägre kostnad.

Ett liknande mönster kan ses i administrativt tungt säkerhetsarbete, där omfattande manuella kontroller, godkännanden och rutiner införs för att minimera risk. Dessa åtgärder kan ge en viss riskreduktion, men kräver stora mängder arbetstid och skapar friktion i verksamheten. Skadekostnaderna påverkas ofta marginellt, medan skyddskostnaderna ökar kraftigt.

Överdrivet skydd uppstår ofta när samma säkerhetskrav införs generellt i hela verksamheten, i stället för selektivt där de gör nytta. Alla system, lokaler eller processer omfattas av samma höga skyddsnivå, oavsett om de är verksamhetskritiska eller inte. Detta leder till höga skyddskostnader och ökad administrativ belastning, samtidigt som delar av skyddet inte bidrar till att minska relevanta risker.

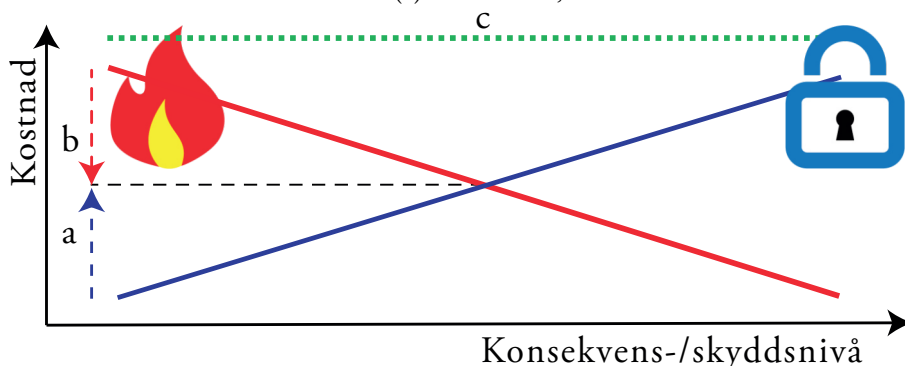
Redundans är i många fall en effektiv metod för verksamhetskritiska tillgångar, men kan bli överdriven när den införs utan tydlig analys. Ett exempel är när flera parallella system eller resurser införs, trots att verksamheten i praktiken saknar förmåga att använda dem vid en störning. Om organisationen inte har rutiner, utbildning eller bemanning för att faktiskt utnyttja redundansen blir den en kostsam försäkring utan verklig effekt på tillgänglighet eller skadekostnader.

Gemensamt för överdrivna skyddsåtgärder är att skyddet saknar proportionalitet i förhållande till tillgångarnas värde, hotbildens karaktär och konsekvensernas omfattning. Skyddsnivån drivs inte av aktuell riskanalys, utan av historik, rädsla, enskilda incidenter eller organisatorisk tröghet. Skyddet blir svårt att anpassa, dyrt att vidmakthålla och i vissa fall direkt hämmande för verksamheten.

Ur ett lönsamhetsperspektiv är överdrivna skyddsåtgärder det minst önskvärda tillståndet i modellen. Skyddet fungerar i någon mening, men utan att skapa ekonomiskt värde. Lönsam säkerhet kräver därför inte bara förmågan att förstärka skyddet när hotbilden ökar, utan också förmågan att justera, förenkla eller avveckla skydd när hotbilden minskar. Att våga växla ned skyddsnivån på ett kontrollerat och genomtänkt sätt är en central del av ett moget och lönsamt säkerhetsarbete.

Kompensatoriska skyddsåtgärder

Teoretiskt sett kan minskade skadekostnader och ökade skyddskostnader ta ut varandra, vilket innebär att skyddet inte blir lönsamt. Exempelvis om vi eftersträvar maximal säkerhet för att undgå alla skador. Vi utgår från att en högre skyddsnivå leder till en högre skyddskostnad (a). Ju högre skyddsnivå desto färre skador och lägre skadekostnader (b). Om skyddskostnaden ökar lika mycket som skadekostnaden minskar förblir totalkostnaden (c) oförändrad, *break-even* och är inte lönsamt.



Kompensatoriska skyddsåtgärder är åtgärder som reducerar skadekostnader i ungefär samma omfattning som skyddskostnaderna ökar. Säkerheten förbättras, men den totala kostnaden för verksamheten förblir oförändrad, vilket innebär att åtgärderna inte leder till lönsamhet.

Ett vanligt exempel är överdimensionerad bemanning. Efter en incident väljer organisationen att öka antalet väktare eller säkerhetspersonal. Skadorna minskar, men personalkostnaderna ökar i motsvarande grad. Resultatet blir ett fungerande skydd, men utan ekonomisk nettoeffekt.

Ett annat exempel är tekniska skydd som överlappar varandra utan tydlig koppling till hotbilden. Flera larmsystem eller övervakningslösningar installeras för samma objekt, trots att hotbilden inte motiverar nivån av redundans. Skadekostnaderna minskar marginellt, medan investerings- och driftskostnaderna ökar lika mycket.

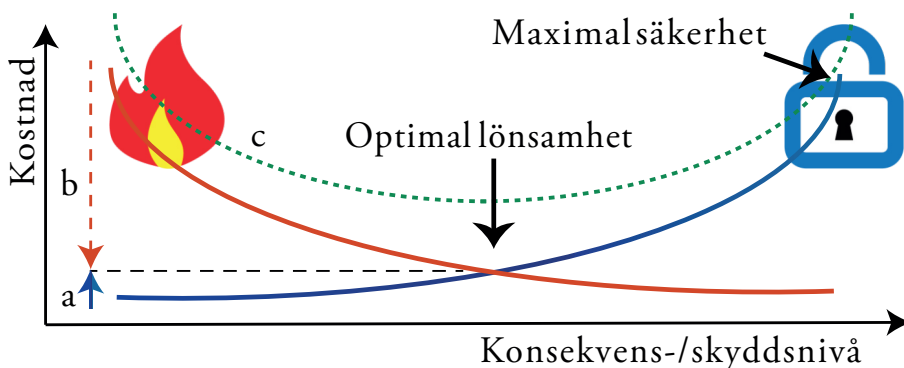
Även mycket hög skyddsnivå överallt i verksamheten är ett kompensatoriskt mönster. När alla områden ges samma skydd, oavsett om de är verksamhetskritiska eller inte, blir skyddskostnaderna höga samtidigt som en del av skyddet inte bidrar till att minska relevanta risker.

Slutligen förekommer kompensatoriska åtgärder i administrativt tungt säkerhetsarbete, där manuella kontroller och rutiner ersätter mer ändamålsenliga lösningar. Riskerna minskar, men arbetstiden och därmed kostnaderna ökar i samma takt.

Gemensamt för dessa exempel är att säkerhetsåtgärderna fungerar ur ett skyddsperspektiv, men skapar inte något ekonomiskt överskott. Skyddet kompenserar för skadorna, men totalkostnaden förblir oförändrad, ett klassiskt *break-even*-läge.

Optimala skyddsåtgärder

För att uppnå lönsamhet bör man sträva efter **optimal lönsamhet** snarare än **maximal säkerhet**. Optimal lönsamhet innebär att skador förebyggs i den utsträckning det är ekonomiskt motiverat. Det är sällan lönsamt att försöka förebygga alla tänkbara skador till varje pris. I vissa fall är det mer kostnadseffektivt att acceptera en kvarvarande risk och hantera konsekvensen när den inträffar.



Optimal lönsamhet uppnås när skyddskostnaden (a) minskar skadekostnaden (b) mer än vad skyddskostnaden ökar, så att den totala kostnaden (c) blir så låg som möjligt. Fokus ligger inte på att minimera vare sig skyddskostnader eller skadekostnader var för sig, utan på att optimera helheten. För att uppnå detta behöver skyddskostnaderna optimeras genom att kombinera flera olika åtgärder på ett genomtänkt sätt, till exempel genom att:

- prioritera kostnadseffektiva skyddsåtgärder, där man börjar med billiga och effektiva åtgärder och är återhållsam med de dyraste och minst effektiva,
- tillämpa skydd i flera lager med kompletterande skyddsåtgärder,
- minimera risken för att en enskild komponent eller åtgärd blir en kritisk svaghet som äventyrar hela skyddet,
- skapa ett balanserat skydd med jämn skyddsnivå runt hela objektet,
- utforma skyddet baserat på faktisk prestation och skyddseffekt, snarare än enbart funktion eller teknisk lösning,
- införa skyddsåtgärder i rätt ordning, där upptäckt sker tidigt så nära perimetern som möjligt och följs av tillräcklig fördröjning fram till det skyddsvärda objektet, så att insats hinner fram för att avbryta och ingripa,
- säkerställa löpande underhåll av skyddsåtgärderna för att förhindra att skyddseffekten försämras över tid.

Bokserien Lönsam säkerhet

Bokserien Lönsam säkerhet beskriver hur säkerhetsarbetet kan integreras i verksamhetens ledning och samtidigt nå ut i hela organisationen. Böckerna bygger på samma modell men behandlar säkerhetsarbetet ur olika perspektiv, från ledningens beslut och verksamhetens analyser till genomförande, säkerhetsåtgärder och uppföljning.

Gemensamt för böckerna är synen på säkerhet som en del av verksamhetens styrning och värdeskapande. Syftet är att utveckla ett effektivt och lönsamt säkerhetsarbete som skyddar verksamhetens tillgångar, utvecklar dess förmåga och bidrar till att verksamheten kan nå och överträffa sina mål.

Böckerna kan användas var för sig, men tillsammans skapar de ett gemensamt arbetssätt för ledning, chefer, säkerhetsansvariga, projektledare och andra delar av verksamheten.

Metodboken – förstå och fatta beslut. Metodboken beskriver modellen för Lönsam säkerhet och förklarar sambanden mellan verksamhetens tillgångar, hotbild, konsekvenser, säkerhetsåtgärder, organisation, investeringar, effektivitet och lönsamhet. Boken ger den teoretiska och metodmässiga grunden för att styra säkerhetsarbetet utifrån verksamhetens mål.

Arbetsboken – analysera och välja. Arbetsboken omsätter modellen i praktiskt arbete. Den leder verksamheten steg för steg genom analysen av tillgångar, hotbild, konsekvenser, metoder, organisation, effektivitet, investeringar och lönsamhet. Resultatet är ett strukturerat beslutsunderlag för val och prioritering av åtgärder.

Projektboken – genomföra förändringen. Projektboken tar vid när verksamheten har beslutat vad som ska förändras. Den beskriver hur behov och krav omsätts till fungerande lösningar genom projektering, upphandling, genomförande, kvalitets-säkring, överlämning och förvaltning. Målet är inte bara en genomförd leverans utan en fungerande verksamhetsförmåga.

Säkerhetsboken – förstå säkerhetsarbetet. Säkerhetsboken ger den breda kunskap som behövs för att förstå och utveckla verksamhetens säkerhet. Den behandlar säkerhetsledning, riskhantering och olika säkerhetsområden samt verksamhetens kontinuitet, resiliens och krishantering. Boken fungerar som seriens kunskapsbas och fördjupar de områden och lösningar som aktualiseras när modellen tillämpas.

Tillsammans ger böckerna kunskap, metoder och arbetssätt för att föra säkerhetsarbetet från ledningens beslut ut i hela verksamheten och utveckla en säkerhet som skapar lönsamhet och bidrar till att verksamheten kan nå och överträffa sina mål.



Hur leder man säkerhetsarbete så att det verkligen skapar värde?

Säkerhet handlar om att verksamheten ska kunna nå sina mål utan oönskade händelser som försämrar förutsättningarna. Lönsam säkerhet handlar om att göra detta så ekonomiskt som möjligt genom att minska skadekostnader, använda resurser där de ger störst effekt och samtidigt bidra till verksamhetens värdeskapande.

Metodboken beskriver modellen för lönsam säkerhet och visar hur säkerhetsarbetet kan integreras i verksamhetens ledning och styrning. Tillgångar, hotbild, konsekvenser, metod, organisation, effektivitet, investeringar och lönsamhet kopplas samman till ett gemensamt beslutsunderlag.

Boken beskriver bland annat:

- hur säkerhetsarbetet utgår från verksamhetens mål och tillgångar
- hur hot och konsekvenser påverkar risk och prioriteringar
- hur metod och organisation påverkar skyddseffekten
- hur investeringar i säkerhet kan bedömas ekonomiskt
- hur effektivitet och lönsamhet kan mätas
- hur säkerhetsarbetet kan styras och utvecklas över tid

Metodboken riktar sig till chefer, ledningsgrupper och andra beslutsfattare som behöver förstå vad som behöver göras och varför. Den ger grunden för ett säkerhetsarbete som skyddar verksamheten och samtidigt bidrar till att den kan nå och överträffa sina mål.

www.securitymanager.se

www.lönsamsäkerhet.se

