Berberovic, Boris
boris.berberovic@skane.se

YTTRANDE

Datum 2024-05-14
Ärendenummer 2024-POL000115

Remiss Delbetänkandet Nya regler om cybersäkerhet SOU nr 18 2024

Region Skåne har beretts möjlighet att yttra sig över Delbetänkandet Nya regler om cybersäkerhet SOU nr 18 2024 och nedan följer en sammanställning av regionens synpunkter på utredningens förslag och bedömningar.

En viktig utgångspunkt för Region Skånes yttrande på denna remiss utgörs av de begrepp som diskutera i bilaga 1. Förslag till utredarna och återkopplingen till remissen är att tydligt definiera de olika begreppen, deras samspel och hur de relaterar till varandra i syfte att tydliggöra begreppen, motverka feltolkningar och förvirring vad informationssäkerhet och informationssäkerhetsområdet är, vad begreppen it-säkerhet och cybersäkerhet är utifrån begreppens korrelation inom området.

Rekommendationen är att fortsätta använda internationell standard ISO 27000-serien som en utgångspunkt och ramverk för arbetet med informations- och cybersäkerheten eftersom det anvisas av EU, Sverige och svenska tillsynsmyndigheter, internationella och svenska leverantörer samt andra organisationer såsom revisorsorganisationer som utövar tillsyn åt interna revisionsfunktioner.

Tydlighet i begreppsdefinitioner, deras innebörd och samspel kan förutom att underlätta lagens implementering också ha stor bäring och påverkan på att öka mognaden inom framför allt den offentliga Sverige.

Flera tillsynsmyndigheter kan försvåra en samsyn inom regionen
Inledningsvis så kommer Region Skåne på grund av den nya lagstiftningen ha verksamhetsutövare i flera sektorer, och med utredningens förslag kommer olika tillsynsansvariga (tex. för regioner kan det handla om MSB, Läkemedelsverket, IVO) i vissa fall meddela föreskrifter med sektorspecifika krav. Region Skåne har en sammanhållen ledning och styrning av informationssäkerhetsarbetet via Koncernkontoret och CISO rollen där regionala övergripande riktlinjerna tas fram för att regionen ska ha en samsyn i detta arbete. Det kan bli en utmaning att MSB inte meddelar förskrifter med grundläggande krav på säkerhet, och att tillsynsansvarig kompletterar vid behov med sektorsanpassade krav; speciellt i frågan om en sammanhållen tillämpning av krav då dessa kan bli olika beroende på vilken sektor och tillsynsansvarig som är kravställare. Särskilt som förslaget

är att kraven inte ska anges för detaljerat då det ankommer på tillsynsmyndigheten att anpassa kraven till respektive sektor.

Därtill har en av Region Skånes största förvaltningar, Skånes universitetssjukhus (SUS) konstaterat att SUS skulle kunna anses bedriva verksamhet inom flera sektorer som träffas av regleringen och då skulle en verksamhetsutövare ha flera tillsynsansvariga. För att undvika en situation där flera myndigheter är behöriga att bedriva tillsyn över samma verksamhetsutövare föreslås i utredningen en begränsning; om tillsyn över en verksamhetsutövare utövas av fler än en tillsynsmyndighet ska respektive tillsynsmyndighet inte utöva tillsyn gällande den del av verksamheten som anges som en annan tillsynsmyndighets tillsynsområde. Region Skåne instämmer i utredningens bedömning att ett samlande av tillsynsansvaret i en central tillsynsmyndighet skulle bli en mycket omfattande uppgift för en myndighet. I relation till föreskriftsrätten bedöms det dock, med det föreslagna systemet och fördelningen av ansvar, finnas en risk för att verksamhetsutövare som ska tillämpa olika föreskrifter för respektive sektor skulle kunna träffas av motstridiga krav. En dämpande omständighet är förslaget att utarbeta en vägledning till stöd för tillsynsmyndigheternas föreskriftsarbete så att föreskrifterna blir likvärdiga, som enligt Region Skåne blir extra viktigt. Dock ser vi fortfarande att det finns riskerar för att det blir kostnadsdrivande och kan medföra en risk för oförenliga krav av skäl som ges ovan, samt blir administrativt betungande för verksamhetsutövarna.

Enligt utredningens förslag ska verksamhetsutövare informera sina kunder om de anses påverkade av en betydande incident samt ges information om avhjälpande åtgärder vilket gäller även för ett betydande cyberhot. Utredningen föreslår att detta ska ske efter senast 72 timmar i samband med incidentanmälan, och som sanktionering ska tillsynsmyndigheten kunna meddela om föreläggande som kan förenas med vite. Återigen kan detta få negativa effekter för Region Skåne, avseende hanteringen tex. genom att informera kund (patient, resenär, besökare) som genom sin storlek och komplexitet har stora utmaningar med kommunikation till kund ska ske på ett strukturerat sätt inom angiven tid, om föreskrifterna från de olika tillsynsmyndigheter inte harmoniseras.

Ett annat perspektiv är den finansiella och resursmässiga merkostnad som Region Skåne kan se om vissa funktioner inte kan samordnas i en regional enhet; om det blir enligt utredningens förslag dvs. att det ska vara tillsynsmyndigheterna som får meddela föreskrifter om riskhanteringsåtgärder, systematiskt och riskbaserat informationssäkerhetsarbete samt utbildning om riskhantersåtgärder. Då finns en risk att Region Skånes ambition om en central sammanhållen styrning av det systematiska informationssäkerhetsarbetet inte går att upprätthålla på ett strukturerat och (kostnads)effektivt sätt.

Ökade krav på verksamhetsutövarna
Det kan noteras i sammanhanget att det redan inom en rad områden finns regleringar som innefattar exempelvis anmälningsplikt och att den nya regleringen kommer innebära tillkommande skyldigheter. Vad gäller anmälningspliktiga personuppgiftsincidenter enligt artikel 33 EU:s allmänna dataskyddsförordning

kommer händelsen, om personuppgiftsincidenten räknas som en betydande incident enligt NIS2 och har påverkat eller kan påverka fysiska personer genom att vålla betydande materiell eller immateriell skada, även rapporteras till MSB (CSIRT-enheten) inom 24 timmar efter att verksamhetsutövaren fått kännedom om den betydande incidenten.

Ett tillkommande rapporteringskrav på 24 timmar, jämfört med 72 timmars rapporteringskrav till IMY, kommer att ställa utökade krav på verksamhetsutövare som behandlar stora mängder känsliga och skyddsvärda uppgifter, särskilt mot bakgrund av NIS2 direktivets definition av begreppet incident, jämfört mot nuvarande definition i lag om informationssäkerhet för samhällsviktiga och digitala tjänster.

Region Skåne delar inte utredningens bedömning att de tillkommande kostnaderna för de offentliga verksamhetsutövarna bör finansieras inom den befintliga ramen. Region Skåne delar i sig utredningens bedömning att det är rimligt att offentliga verksamhetsutövare vidtar grundläggande säkerhetsåtgärder, men anser att utredningen undervärderar konsekvenserna för offentliga verksamhetsutövare i relation till de tillkommande kraven, särskilt med beaktande av de nuvarande resurserna som finns att tillgå. I sammanhanget bör även påpekas att det finns en generell kompetensförsörjningsproblematik inom informationssäkerhetsområdet som särskilt drabbar offentliga aktörer och är kostnadsdrivande. Kostnadsökningen till följd av regleringen bedöms bli betydande för offentliga verksamhetsutövare när hela verksamheten kommer omfattas av direktivets krav om riskhanterings- och rapporteringskrav.

Region Skåne delar inte utredningens bedömning att färre incidenter, till följd av de ökande kraven och på sikt förmodade förbättrade säkerheten, ger lägre kostnader. Region Skåne anser att detta är en förenklad bild som inte tar hänsyn till komplexiteten av det arbete som krävs för respektive verksamhetsutövare, särskilt utifrån behovet av ett kontinuerligt arbete i en rörlig omvärld där riskerna förändras i takt med den tekniska utvecklingen.

Tillsyn för utlokaliserade tjänster och IT-miljö
En tillsynsmyndighet som utövar tillsyn över en verksamhetsutövare ges rätten att få del av de upplysningar eller handlingar i den uträckning som behövs för tillsynen, detta gäller även fysiskt tillträde till områden, lokaler och andra utrymmen där verksamhet bedrivs som omfattas av lagen. I en situation där tillsynsmyndigheten begär tillgång till uppgifter, handlingar och information för att kunna utöva en tillsyn, kan dessa uppgifter utlämnas av verksamhetsutövaren. Det är ej tydligt i utredningen om tillsynen och rätten till tillträde till områden, lokaler och andra utrymmen även gäller driftsleverantören i de fall där tjänster och/eller IT-driften är utlokaliserad. Här skulle Region Skåne föreslå ett förtydligande från utredningen om vad som gäller när verksamheter som omfattas av lagen har utlokaliserad IT-drift.

Detsamma gäller för utredningens förslag att tillsynsmyndigheten får genomföra sårbarhetsskanning hos verksamhetsutövaren, vilket lyfter frågan över vad det

har för konsekvenser för en verksamhetsutövare som har en utlokaliserad IT-driftmiljön samt för leverantören av den utlokaliserade IT-miljön.

Sekretesskydd för information i systemstöd
Utredningen föreslås i sin analys om befintliga bestämmelser i OSL tillgodoser NIS2-direktivets även inkludera sekretesskyddet för information i systemstöd. Region Skånes bedömning är att information både i och om tekniska system i de flesta fall omfattas av sekretess enligt Offentlighets- och sekretesslagen 18 kapitlet 8 § eller 13 §.

Sekretess enligt dessa nämnda paragrafer begränsas inte i tid, men regleras av rakt skaderekvisit, det vill säga det föreligger en presumtion för att informationen är offentlig om det skulle saknas konkreta aspekter som till exempel ett faktiskt hot.

Region Skånes bedömning är det finns behov av att se över sekretessregleringen gällande information som är direkt hänförlig till ovanstående.

Carl Johan Sonesson
Ordförande

Lars-Åke Rudin
Regiondirektör

Boris Berberovic
Boris.berberovic@skane.se

YTTRANDE

Datum 2024-05-14
Ärendenummer 2024-POL000115

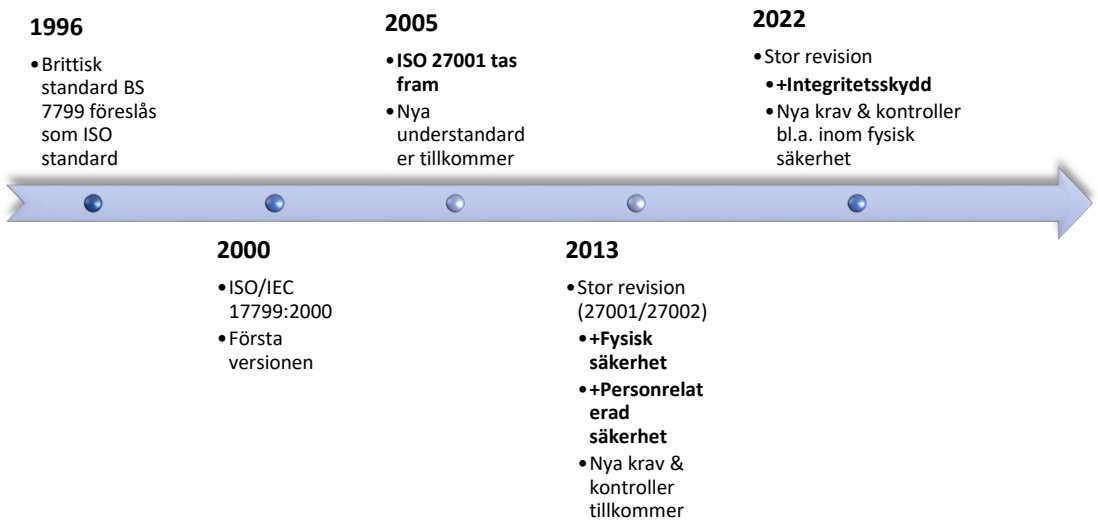
Remiss Delbetänkandet Nya regler om cybersäkerhet SOU nr 18 2024

Bilaga 1

Tydliggörande av begrepp, definitioner och samspel

Informationssäkerheten och därefter it-säkerheten och cybersäkerheten är relativt nya begrepp. Det kan råda förvirring kring vad som ingår i dessa begrepp vilket påverkar mognaden inom informationssäkerhetsområdet. Det existerar en uttalad brist på spetskompetens kombinerat med stark konkurrens mellan den privata och offentliga sektorn där privata sektorn erbjuder ofta högre löner och snabbare utvecklingstakt samt mognare organisationer och ansvarsområden. Privata och offentliga sektorer kan dessutom ha olika syn på begreppen beroende på var dessa sektorer vanligtvis hämtar kompetensen ifrån – ofta till nackdel för den offentliga sektorn där mognaden enligt olika rapporter och utredningar är lägre.

Det är mycket som har hänt och fortsätter att hända med informationssäkerhetsområdet under relativt kort tid. Området har expanderat från att från början handlat om de organisatoriska och tekniska krav och åtgärder till att omfatta de fysiska- och personrelaterade delområden. Personrelaterat- kallas också för administrativt delområde av MSB - Myndigheten för Samhällsskydd och Beredskap. Integritetsskyddet är det senaste tillskottet som tillkom år 2022 enligt figur nedan.



MSB, FRA, Försvarsmakten, Säkerhetspolisen, FMV, PTS och Polisen som samverkar via sajten www.informationssakerhet.se som ska ge stöd för systematiskt arbete med informationssäkerhet i organisationer beskriver informationssäkerheten under fliken ”Om informationssäkerhet” som:

Information är en grundläggande byggsten i en organisation, på samma sätt som medarbetare, lokaler och utrustning. Genom ett systematiskt arbete med informationssäkerhet kan organisationer öka kvaliteten i och förtroendet för sin verksamhet. Att utgå från etablerade standarder i arbetet med informationssäkerhet ökar chansen att lyckas väl.

Arbetet med **informationssäkerhet omfattar att införa och förvalta administrativa regelverk så som policys och riktlinjer, tekniskt skydd med bland annat brandväggar och kryptering samt fysiskt skydd med till exempel skal- och brandskydd.** Det **handlar om att ta ett helhetsgrepp** och skapa ett fungerande långsiktigt arbetssätt för att ge organisationens information det skydd den behöver.

Begreppsdefinitionerna och själva frågan avseende ”Vad är informationssäkerhet?” är viktiga utifrån ansvarsfördelning över vilken roll inom offentliga organisationer, i synnerhet de regionala- och kommunala organisationer, som har eller bör ha det yttersta ansvaret. ISO 27000 serien, i synnerhet ISO 27001 som är en svensk standard SS-EN ISO/IEC 27001:202 definierar Ledningssystem för Informationssäkerhet där Informationssäkerhet, Cybersäkerhet och integritetsskydd ingår. ISO 27002, som ”SVENSK STANDARD SS-EN ISO/IEC 27002:2022 Informationssäkerhet, cybersäkerhet och integritetsskydd – Kontroller av informationssäkerhet (ISO/IEC 27002:2022)”, ungefär som sajten www.informationssakerhet.se delar upp informationssäkerhetsområdet i fyra

delområden enlig säkerhetsåtgärdstyp: organisatoriskt, personrelaterat, fysiskt och tekniskt.

Det förekommer ofta, framför allt på myndigheter, stora begreppsförvirringar kring vad begreppen informationssäkerhet, cybersäkerhet och it-säkerhet är. Informationssäkerheten som omfattar helheten definieras då felaktigt som enbart det organisatoriska delområdet som är en viktig men begränsad del av informationssäkerhetsområdet. På grund av mycket längre erfarenhet med att jobba med informationsstyrning och framför allt informationshantering inom offentliga organisationer, kan offentliga organisationer tolka den organisatoriska delen av informationssäkerheten som en informationshanteringsfråga.

Cybersäkerheten å andra sidan kan oftast tolkas som en it-säkerhetsfråga då cybersäkerheten kan på grund av begreppsförvirringen ofta förväxlas eller utbytas med it-säkerhet och då placeras under styrning och ledning av IT avdelningar. Därmed kan det uppstå ett gap och ett vakuum som resulterar i organisatoriska-, strukturella- och i slutligen säkerhetsmässiga risker som motverkar enhetlig samordning och ledning i frågan och förstärker arbete i stuprör.

Många organisationer har idag Informationssäkerhetschefer eller CISO (hädanefter kallas bara CISO) roller med varierande grad av stödjande eller supporterande organisation som kan vara linje-, matris- eller hybridbaserad. I mindre organisationer, där CISO kan ofta vara ensamma i sin roller, kan rollerna i regel påverka den organisatoriska delen av informationssäkerhetsområdet medan ansvaret för de resterande tre delområden dvs. personrelaterat, fysiskt och tekniskt effektivt kan hamna på andra roller – oftast på redan befintliga roller såsom säkerhetschef/säkerhetsskyddschef för den fysiska, IT chefs/ansvarig eller it-säkerhetsansvarig för den tekniska och slutligen på HR chef för den personrelaterade delen. Mandatet att samordna ett så stort område enligt definitionen från www.informationssakerhet.se är en bred uppgift. Större eller mognare organisationer har CISO roller med uppdrag att styra och leda området men även där kan finnas, på grund av historiken och begreppsförvirringen, stora organisatoriska eller strukturella gap. Frågan lyfts om organisationer och deras ledningar, i synnerhet inom den offentliga Sverige, har förståelse och insikt över vilken strategisk vikt informationssäkerhetsområdet har som beror på definitionen av vad informationssäkerhetsområdet är, och vilka roller har ansvar för att styra, leda eller samordna beroende på av ledningen valt mandat.

EU förordningar och cybersäkerhetslagen har möjlighet att skapa eller förtydliga de insikterna och kan bli ett viktigt verktyg för att fokusera och lyfta frågan. Dock kallas lagen just för cybersäkerhetslagen och med det finns en stor chans

att med tanke på de definierande begrepp eller tolkade begreppsuppfattningar att cybersäkerhet läggs närmast eller blir en del av it-säkerheten där frågan då nästan per automatik kan anses tillhöra till IT avdelningarna eller till förvaltningar som har IT som ansvarsområde.

I ”EU:s cybersäkerhetsakt – kompletterande nationella bestämmelser om cybersäkerhetscertifiering”, SOU 2020:58 under kapitel 3.3, ”Styrning av informations- och cybersäkerhet” står följande:

Styrning av informationssäkerhet handlar om att upprätta strukturer och politik för att säkerställa konfidentialitet, integritet och tillgänglighet för data. **Det är mer än en teknisk fråga**. Styrning av cybersäkerhet omfattar alla slags cyberrelaterade hot, inbegripet målinriktade, sofistikerade angrepp, överträdelser eller incidenter som är svåra att upptäcka eller åtgärda.

I ”Förslag till lag om cybersäkerhet” under 2 § står definitioner eller hänvisningar till definitioner vad cybersäkerhet är. Definitionen hänvisar till Cybersäkerhetsakten.

Cybersäkerhetsakten nämner följande under kapitel 2.1 Bakgrund:

Genom att kontrollera och certifiera produkter, tjänster och processer kan man göra dem säkrare och därigenom även öka förtroendet för dessa. Det finns certifieringsordningar inom ett stort antal områden, bl.a. inom informationssäkerhetsområdet men även på områden som lednings-, miljö- och trafikledningssystem samt inom hälso- och sjukvård.

Samt även under underkapitlet ”Nationell informations- och cybersäkerhetsstrategi”

För att informationshantering och it-användning i samhället ska kunna utvecklas på ett tryggt och säkert sätt krävs att alla aktörer har en **helhetssyn på informationssäkerhet**, som ska vara en självklar och integrerad del i allt arbete på alla nivåer i samhället.

Slutsatsen av ovanstående kan vara att det finns ett antal internationella ledningssystem för miljö, ledning samt informationssäkerhet och att informationssäkerhetsområdet är det helhetsperspektivet som omfattar de andra begreppen it-säkerhet och cybersäkerhet.

Cybersäkerhetsakten i artikel 2.1 punkt 1 definierar cybersäkerheten som:

1. cybersäkerhet: all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot.

I utredningen ”Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem, betänkandet kring cybersäkerhetsutredningen”, SOU 2021:63 står följande under kapitel 7.2:

Begreppet informationssäkerhet infördes i 1996 års lagstiftning om säkerhetsskydd som en ersättning till det tidigare begreppet sekretesskydd.

…

Informationssäkerhet enligt regleringen om säkerhetsskydd innebär åtgärder av olika slag för att skydda information som är av betydelse för säkerhetskänslig verksamhet. Sådan information förekommer i olika miljöer och verksamheter och hanteras och används på flera olika sätt. Därför måste säkerhetsskyddsåtgärderna anpassas för att passa för dessa skiftande förutsättningar. Uppgifternas form saknar i sammanhanget betydelse och åtgärderna måste avse såväl elektroniskt lagrade och kommunicerade uppgifter som uppgifter på papper samt uppgifter som kan läsas ut ur t.ex. bilder eller materiel.

Man kan beskriva informationens livscykel från det att den skapas till det att den upphör eller förstörs och att utifrån denna beskrivning identifiera moment som har betydelse för säkerheten. Dessa moment i informationshanteringen kan skyddas genom administrativa, fysiska eller tekniska säkerhetsskyddsåtgärder eller genom en kombination av dessa. För att beskriva åtgärdernas karaktär kan de indelas i tre kategorier:

– administrativ informationssäkerhet,

– it-säkerhet,

– kommunikationssäkerhet.

De ovanstående kategorier har följande beskrivningar i utredningen:

Administrativ informationssäkerhet

Till de administrativa informationssäkerhetsåtgärderna hör åtgärder som tar sikte på rutiner, arbetsflöden och arbetsledning. Här kan nämnas bestämmelser om registrering, distribution, kopiering, kvittering och inventering av handlingar som innehåller säkerhetsskyddsklassificerade uppgifter. Ett exempel på en sådan bestämmelse är att handlingar som placerats i informationssäkerhetsklass konfidentiell eller högre ska kvitteras av den som tar del av handlingen. En för säker-

hetsskyddet central fråga är reglerna om behörighet till säkerhetsskydds-klassificerade uppgifter. Behörighetskriteriet innebär att en person för att vara behörig till hemliga uppgifter ska vara pålitlig från ett säkerhetsperspektiv, ha relevanta kunskaper om säkerhetsskyddet och ha behov av uppgifterna för sin tjänst eller för sitt uppdrag.

It-säkerhet

It-säkerheten innefattar regler om handhavande och rutiner för in-formationssystem (nätverks- och informationssystem) jämte tekniska krav på säkerhetsfunktioner i systemen och komponenter. För att även säkerställa att tillgängligheten är i enlighet med verksamhetens krav bör informationssystem som används i säkerhetskänslig verk-samhet vara föremål för kontinuitetsplane-ring. Säkerhetskopiering är också en viktig åtgärd som ger ett skydd i termer kring tillgänglighet och riktighet. Till it-säkerheten hör även bestämmelser som rör krav på säkerhetsgodkännande av it-system inför driftsättning. Ett exempel på en säkerhetsskyddsbestämmelse inom it-säkerheten är att lag-ringsmedia som innehåller säkerhetsklassificerade uppgifter ska för-varas och hanteras på samma sätt som säkerhetsskyddsklassificerade handlingar. Åtgärder som behö-righetskontroll och skydd mot obehörig avlyssning är också viktiga beståndsde-lar av it-säkerheten.

Kommunikationssäkerhet

Termen signalskydd används för att beskriva det i huvudsak krypto-grafiska skyddet för information i s.k. signalskyddssystem. Bestämmelser om signal-skydd och kryptografiska funktioner förekommer i dag i flera olika författning-ar. Försvarsmakten har i uppgift att leda och bedriva militär säkerhetstjänst samt leda och samordna signal-skyddstjänsten. Det innebär arbete med säkra krypto-grafiska funktioner som är avsedda att skydda skyddsvärd information samt även biträda Regeringskansliet i frågor som rör kryptoverksamhet och annan signalskyddsverksamhet. Bestämmelsen om vad säkerhetsskyddslagen ska skydda mot.

Utredningen ”Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem, betänkandet kring cybersäkerhetsutredningen”, SOU 2021:63 är från år 2021 medan den senare upplagan av ISO 27002:2023, som är från 2023 delar upp informationssäkerhetsområdet inom organisatoriskt, fysiskt, tekniskt och personrelaterat baserat på uppdelning av typer av skyddsåtgärder.

Ovanstående kan påvisa att kategorierna är inte uppdaterade eller anpassade åt den ena eller andra hållet, baserat på internationella tillsynsmyndigheternas- eller lagstiftarens definition(er).

Utredningen ”Sveriges säkerhet – behov av starkare skydd för nätverks- och informationssystem, betänkandet kring cybersäkerhetsutredningen”, SOU 2021:63 definierar följande begrepp i kapitel 2.4 Definitioner

Utredningen behandlar frågor och verksamheter som rör begrepp som digitalisering, cyber, informations- och cybersäkerhet, m.m. Begrepp som informationssäkerhet, it-säkerhet och cybersäkerhet förekommer i många olika sammanhang, såväl nationellt som internationellt.

Figur 2.1 Av figuren framgår hur begreppen cybersäkerhet, it-säkerhet och informationssäkerhet förhåller sig till varandra