IT-incidenter på statliga myndigheter

Orsaker till utebliven rapportering

Ann-Sofie Stenérus Dover, Johan Bengtsson och Matilda Olsson

FOI-R--4815--SE

Februari 2020

FOI

Ann-Sofie Stenérus Dover, Johan Bengtsson och Matilda Olsson

IT-incidenter på statliga myndigheter

Orsaker till utebliven rapportering

Titel	**IT-incidenter på statliga myndigheter – Orsaker till utebliven rapportering**
Title	IT incidents at state agencies **–** Causes of missing reporting and police reporting
Rapportnr	FOI-R--4815--SE
Månad	Februari
Utgivningsår	2020
Antal sidor	124
ISSN	1650-1942
Kund	Justitiedepartementet
Forskningsområde	Informationssäkerhet
FoT-område	Inget FoT-område
Projektnr/Project no	A1190809
Godkänd av	Lars Höstbeck
Ansvarig avdelning	Försvarsanalys

Bild/Cover: Shutterstock/mikeledray

Sammanfattning

Sedan 2016 är det obligatoriskt för statliga myndigheter att rapportera allvarliga IT-incidenter till MSB. Under åren 2016–2018 rapporterade en tredjedel av myndigheterna IT-incidenter, något som MSB bedömer är en underrapportering. Denna studie undersöker anledningar till att myndigheter inte rapporterar inträffade IT-incidenter samt att de inte polisanmäler inträffade IT-incidenter med ursprung i brottsliga gärningar.

Genom en enkät riktad till samtliga rapporteringsskyldiga myndigheter samlade studien information om myndigheternas förutsättningar för IT-incidentrapportering samt deras egen bedömning av potentiella anledningar till utebliven rapportering och polisanmälan.

Analysen av enkätunderlaget visar att det inte finns *en* anledning som förklarar den låga rapporterings- och anmälningsgraden. Nuvarande situation beror istället på flera faktorer som, enskilt och i samspel, bidrar till att rapportering uteblir. Några faktorer som framträder är: bristande interna rutiner för identifiering av IT-incidenter samt rutiner för överföring av sekretessbelagd information, hög arbetsbelastning, svårigheter i att bedöma incidenters allvarlighetsgrad, bristande återkoppling från MSB samt bristande kunskaper rörande rapporteringsskyldigheten. Faktorer för utebliven polisanmälan är framför allt svårigheter i att bedöma allvarlighetsgraden, icke inarbetade rutiner för polisanmälan samt låg upplevd nytta med en polisanmälan.

Rapporteringsskyldiga myndigheter är inte en homogen grupp. Därför är inte alla orsaker bakom utebliven rapportering av IT-incidenter relevanta i samma utsträckning för samtliga myndigheter.

Nyckelord: IT-incidenter, IT-incidentrapportering, rapporteringsskyldiga myndigheter, informationssäkerhet, lägesbild

Summary

Since 2016, it has been mandatory for government agencies to report serious IT incidents to MSB. During the years 2016–2018, one third of the agencies reported IT incidents, which MSB estimates is an under-reporting. This study examines reasons why agencies do not report IT incidents and why they do not report IT incidents originating from criminal acts to the police.

Through a survey directed to all reporting agencies, the study gathered information about the agencies' prerequisites for IT incident reporting as well as their own assessment of potential reasons for not reporting to MSB or the police.

The analysis of the survey data shows that there is no single reason to explain the low reporting rates. The current situation is instead due to several factors that, individually and in collaboration, contribute to the failure of reporting. Some factors that emerge are; lack of internal routines for identifying IT incidents and routines for the transmission of classified information; high workload; difficulties in assessing the severity of incidents; lack of feedback from MSB; and lack of knowledge regarding reporting obligations. Factors for not reporting to the police are, above all, difficulties in assessing the severity; non-established routines for reporting to the police; and low perceived benefit of reporting to the police.

The government agencies are not a homogeneous group. Therefore, not all the reasons behind the failure to report IT incidents are relevant to the same extent to all agencies.

Keywords: IT incidents, IT incident reporting, situational awareness, information security.

Innehåll

1 Inledning

Den 1 april 2016 infördes ett krav på statliga myndigheter under regeringen att rapportera inträffade IT-incidenter till Myndigheten för samhällsskydd och beredskap (MSB). Kravet på myndigheter att rapportera inträffade IT-incidenter återfinns i 20§ i förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap (Justitiedepartementet, 2015b). Enligt denna ska myndigheter till MSB *skyndsamt rapportera IT-incidenter som inträffat i den rapporterande myndighetens informationssystem och som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för, eller som inträffat i tjänster som myndigheten tillhandahåller åt en annan organisation*. Enligt samma förordning 3§ gäller rapporteringskravet samtliga myndigheter under regeringen, med undantag för Regeringskansliet, kommittéväsendet, Säkerhetspolisen, Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt och Totalförsvarets forskningsinstitut.[1]

Syftet med den obligatoriska IT-incidentrapporteringen är, enligt regeringen, att möjliggöra en förbättrad lägesbild över informationssäkerheten i statlig förvaltning (Justitiedepartementet, 2015a). Den förbättrade lägesbilden förväntas ge förutsättningar att vidta rätt skyddsåtgärder samt bidra till att utveckla förmågan att förebygga, upptäcka och hantera IT-incidenter.

För att förordningen om IT-incidentrapportering ska kunna få önskad effekt krävs att myndigheterna rapporterar att allvarliga IT-incidenter har inträffat. MSB gör bedömningen att det finns anledning att tro att myndigheterna inte rapporterar alla allvarliga IT-incidenter. MSB:s årliga sammanställningar av IT-incidentrapporteringen (MSB, 2018; MSB 2019) visar på att bara cirka en tredjedel av myndigheterna rapporterar minst en IT-incident under ett år. Rapporterande myndigheter kan variera mellan åren, men den totala rapporteringsgraden är relativt konstant.[2] Två tredjedelar av myndigheterna rapporterar således inga allvarliga incidenter under ett helt år. Av de IT-incidenter som rapporteras är dessutom andelen som polisanmäls låg. Under

[1] Undantag gäller även för myndigheter som har delar av sin IT-drift utkontrakterad till en ickestatlig aktör och avtalet för detta omförhandlades innan april 2016 då MSB:s föreskrifter om incidentrapportering (9§ MSBFS 2016:2) trädde i kraft.

[2] 2016 och 2017 var 244 myndigheter rapporteringsskyldiga medan det under 2018 var 256. Antalet unika myndigheter som gjort minst en incidentrapport har årligen legat i intervallet 77–87 myndigheter.

2018 polisanmäldes exempelvis endast 11 procent av de rapporterade IT-incidenter som klassades som angrepp.

Sedan förordningen om obligatorisk rapportering av IT-incidenter trädde i kraft har förbättringsarbete pågått för att öka rapporteringen av IT-incidenter samt polisanmälan av de IT-incidenter som har sin grund i en brottslig gärning. MSB har exempelvis utvecklat ett metodstöd, gett återkoppling till myndigheter, genomfört kunskapshöjande insatser och haft översyn av föreskrifterna. Vid årsskiftet 2019/2020 kommer nya reviderade föreskrifter för IT-incidentrapporteringen.

I strävan efter att ytterligare förbättra genomslaget av IT-incidentrapporteringen har Justitiedepartementet uppdragit åt Totalförsvarets forskningsinstitut (FOI) att inom ramen för anslaget Säkerhets- och försvarspolitisk forskning och analys (SOFFA) 2019 genomföra en studie som syftar till att undersöka vad som orsakar den nuvarande rapporteringsgraden och polisanmälningsgraden.

1.1 Målsättning

Uppdraget från Justitiedepartementet inkluderade följande två frågor som i studien har undersökts.

1. Vad kan vara anledning till att myndigheterna inte rapporterar IT-incidenter till MSB?
2. Vad kan vara anledning till att myndigheterna inte polisanmäler IT-incidenter?

Målsättningen med att genomföra studien är att, om möjligt, hitta förklaringar till det av MSB upplevda låga antalet rapporterade IT-incidenter och polisanmälda IT-incidenter. Svar på frågorna förväntas kunna bidra till både Justitiedepartementets och särskilt MSB:s arbete med att uppnå högre rapporteringsgrad och polisanmälningsgrad.

1.2 Målgrupp

Målgruppen för denna rapport är primärt de personer på Justitiedepartementet och MSB som är involverade i arbetet med IT-incidentrapporteringen i enlighet med förordning 2015:1052 (Justitiedepartementet, 2015b). Ytterligare intressenter kan innefatta de rapporteringsansvariga personerna på myndigheterna som omfattas av förordningen.

1.3 Läsanvisning

Rapporten inleds med en beskrivning av det rapporteringsförfarande som de rapporteringsskyldiga myndigheterna förväntas använda (kapitel 2).

Den metod som har använts för att genomföra studien beskrivs i kapitel 3. Metodbeskrivningen ger insikt i det analysramverk som har använts och som låg till grund för den enkät som användes för datainsamling.

I kapitel 4 presenteras ett bearbetat resultat av enkätundersökningen utifrån analysramverkets sex olika områden.

I kapitel 5 görs en sammanvägning av resultaten i form av en diskussion med återkoppling till studiens två ursprungliga frågeställningar om varför myndigheter inte rapporterar respektive polisanmäler IT-incidenter.

I kapitel 6 presenteras studiens slutsatser. Dessutom ges förslag på fortsatta studier.

Inkluderat i rapporten finns även tre bilagor vars innehåll kompletterar innehållet i rapportens kapitel. I Bilaga A återfinns den enkät med tillhörande följebrev som användes i studien. I Bilaga B ges en komplett presentation av resultatet från enkätstudien fråga för fråga. I enkäten gavs de svarande myndigheterna möjligheten att förmedla egna förslag på förändring som de anser att MSB borde genomföra. Dessa förändringsförslag presenteras i Bilaga C.

2 Rapportering av IT-incidenter

Enligt MSB:s föreskrifter (MSBFS 2016:2) om statliga myndigheters rapportering av IT-incidenter ska en IT-incident rapporteras till MSB senast 24 timmar efter att den rapporteringspliktiga incidenten upptäcktes (MSB, 2016c). Rapportering sker genom ifyllandet av ett rapporteringsformulär som via e-post skickas till MSB. För incidentrapporter som bedöms innehålla sekretessbelagda uppgifter, vilket de oftast gör, tillhandahåller MSB en kryptolösning som skydd vid e-postandet. [3]

För att utgöra en komplett IT-incidentrapport ska den enligt MSB:s föreskrifter innehålla:

- en beskrivning av incidenten
- tidpunkt för när incidenten inträffade och när den upptäcktes
- information om huruvida incidenten är pågående eller avslutad
- information om vilken kategori som incidenten tillhör
- myndighetens initiala bedömning av incidentens omfattning och konsekvenser.

Myndigheten ska utöver punkterna ovan även ange en bedömning av sekretess för inlämnade uppgifter. Om en myndighet inte har möjlighet att lämna en rapport enligt ovan inom 24 timmar finns möjlighet att i samråd med MSB få en förlängd rapporteringstid på upp till två veckor efter det att den rapporteringspliktiga incidenten upptäcktes.

[3] Enligt MSB:s årsrapport omfattas huvuddelen av informationen i de inkomna incidentrapporterna av sekretess (MSB 2019, s. 9).

I MSB:s föreskrifter (MSB, 2016c) listas tio olika kategorier av rapporteringsskyldiga IT-incidenter, vilka är:

1. störning i mjuk- eller hårdvara
2. störning i driftmiljö
3. informationsförlust eller informationsläckage
4. informationsförvanskning
5. hindrad tillgång till information
6. säkerhetsbrist i en produkt
7. angrepp
8. handhavandefel
9. oönskad eller oplanerad störning i kritisk infrastruktur
10. annan plötslig oförutsedd händelse som lett till skada.

Det är myndigheterna själva som avgör om en inträffad IT-incident är så pass allvarlig att den ska omfattas av rapporteringsskyldigheten. Som stöd för myndigheternas bedömning har MSB genom CERT-SE[4] tagit fram ett antal exempel på allvarliga IT-incidenter (MSB, 2016a). Därtill finns skriftligt stöd i form av Allmänna råd som tillägg till föreskrifterna, samt ytterligare information på hemsidan för CERT-SE (CERT-SE, u.å.). Myndigheterna kan också vända sig till CERT-SE för att få råd om och operativt stöd i hanteringen av den inträffade IT-incidenten.

När IT-incidentrapporten mejlas till MSB får myndigheten ett automatiskt svar som tackar för rapporteringen och uppmanar myndigheten att polisanmäla incidenten om det kan antas att den har sin grund i en brottslig gärning. Om myndigheten istället redan har polisanmält incidenten är det tillräckligt att MSB får en kopia av polisanmälan som substitut för en ifylld IT-incidentrapport.

För att orientera myndigheter om IT-incidentläget skickar MSB månadsvis ut information baserad på rapporterade incidenter till myndigheternas kontaktpersoner. I akuta lägen kan MSB också skicka ett blixtmeddelande för att informera myndigheterna om inträffade incidenter. MSB lämnar också årligen en rapport till regeringen som sammanställer och analyserar den IT-incidentrapportering som har skett.

En del av de myndigheter som omfattas av kravet på IT-incidentrapportering har inga egna informationssystem. Istället använder myndigheten

[4] CERT-SE är Sveriges nationella Computer Security Incident Response Team (CSIRT) med uppgift att stödja samhället i arbetet med att hantera och förebygga IT-incidenter. Verksamheten bedrivs vid MSB.

informationssystem tillhörandes en så kallad värdmyndighet.[5] Det varierar från fall till fall i vilken omfattning som värdmyndigheten tillhandahåller system som myndigheten nyttjar. Skyldigheten att rapportera IT-incidenter som drabbar myndighetens verksamhet kvarstår även i fallet om det finns en värdmyndighet. En myndighet kan dock komma överens med sin värdmyndighet om hur rapporteringen till MSB ska ske ifall en IT-incident inträffar som drabbar myndighetens och/eller värdmyndighetens verksamhet. Bara för att myndigheter delar samma informationssystem är det inte säkert att en myndighet och dess värdmyndighet drabbas lika vid en inträffad IT-incident.

[5] Regeringen kan bestämma att en myndighet skall agera värdmyndighet åt en nämndmyndighet genom att exempelvis upplåta lokaler och sköta administrativa (som IT-miljö) eller handläggande uppgifter åt nämndmyndigheten. Värdmyndigheten ansvarar inför regeringen för de uppgifter som den skall sköta. Se 18 § myndighetsförordning (2007:515).

3 Metod

För att besvara studiens frågeställningar har information primärt inhämtats genom en enkätundersökning som har skickats ut till samtliga rapporterings-skyldiga myndigheter. Valet föll på en allomfattande enkätundersökning för att kunna fånga in den stora spridningen av myndigheter som den studerade populationen utgör. Därtill har kunskapsunderlaget från enkätundersökningen kompletterats med skriftliga källor från främst MSB.

Utformningen av enkätundersökningen behövde ta hänsyn till att frågor om myndigheters IT-incidentrapportering kan omfattas av sekretess[6]. Mot den bakgrunden har det inte varit möjligt att ställa direkta frågor angående myndigheternas rapporteringshistorik då dessa svar skulle omfattas av sekretess. Det har därför inte varit möjligt att jämföra enkätsvaren från myndigheter som rapporterar in en stor andel IT-incidenter med sådana som inte gör det.

För att hantera balansen mellan att undvika direkta frågor som samlar in ett underlag som omfattas av sekretess, men samtidigt kunna besvara frågeställningen konstruerades ett analysramverk. Analysramverket består av två delar. Den första delen beskriver myndigheternas bakomliggande förutsättningar för att kunna rapportera och polisanmäla allvarliga IT-incidenter. I rapporten har studieförfattarna utgått från att polisanmälan av IT-incidenter kräver motsvarande förutsättningar som rapportering av IT-incidenter till MSB, därav har ett större fokus lagts på frågan om rapportering snarare än polisanmälan.

Den andra delen består av två hypotetiska scenarier som möjliggör för myndigheterna att peka på möjliga orsaker till utebliven rapportering och utebliven polisanmälan utan att svaren blir sekretessbelagda. De hypotetiska scenarierna omfattas inte av sekretess då det handlar om tänkbara situationer snarare än om något som faktiskt har inträffat.

Båda delarna i analysramverket har legat till grund för enkäten.

3.1 Analysramverk och bedömningsgrund

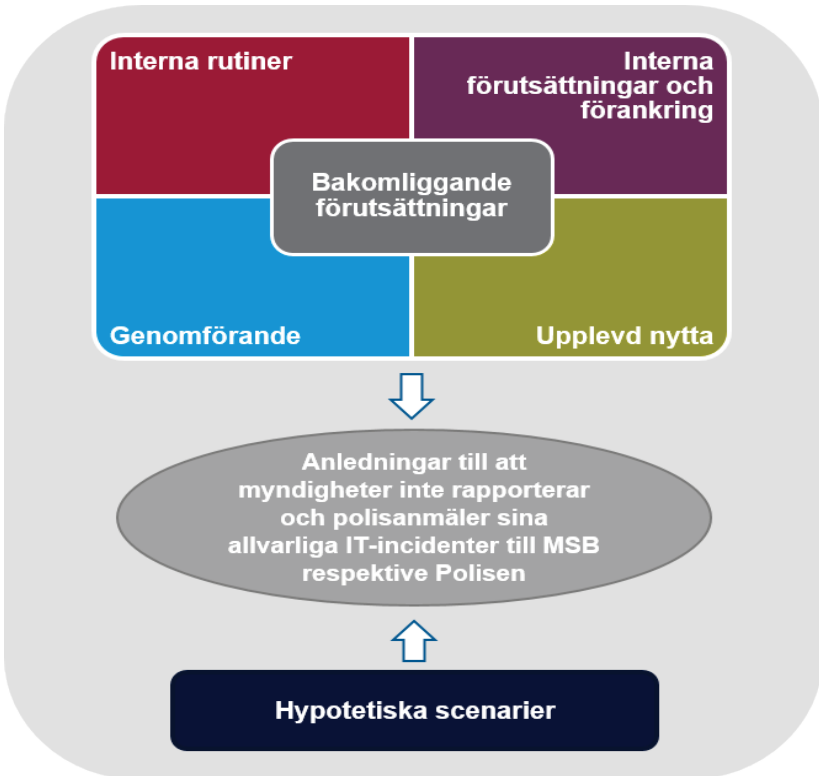
Den del av analysramverket som avhandlar bakomliggande förutsättningar består av fyra områden som av studieförfattarna bedöms vara grundläggande för att möjliggöra ett fungerande rapporteringsförfarande. Bedömningen utgår från kunskap och information som inhämtats genom bland annat rapporter, lagrum,

[6] Offentlighets- och sekretesslag (2009:400), främst 18 kap. 8 § som avser *säkerhets- eller bevakningsåtgärd*.

information från CERT-SE och i diskussion med MSB. Dessa är:

- Interna rutiner (avsnitt 3.1.1)
- Interna förutsättningar och förankring (avsnitt 3.1.2)
- Genomförande (avsnitt 3.1.3)
- Upplevd nytta (avsnitt 3.1.4).

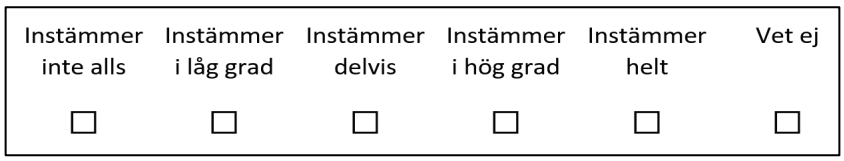
Tillsammans med två hypotetiska scenarier (avsnitt 3.1.5) utgör ovanstående områden det analytiska ramverket.



Figur 1: Visualisering av hur analysramverkets fyra områden och de hypotetiska scenarierna relaterar till studiens två frågeställningar.

I enkäten ställdes frågor inom alla fyra områden som beskriver de bakomliggande förutsättningarna, dvs. för interna rutiner, interna förutsättningar och förankring, genomförande och upplevd nytta. Dessa områden beskrivs mer i detalj i avsnitten 3.1.1-3.1.4. I enkäten efterfrågades också möjliga orsaker till att rapportering inte sker vid två hypotetiska scenarier. Enkäten med dess frågor och scenarier redovisas i helhet i Bilaga A.

I enkäten uppmanades myndigheterna att instämma i en rad påståenden enligt skalan i Figur 2.



Figur 2: Svarsalternativen för hur väl myndigheterna stämde in med ett påstående.

Svarsalternativen i enkätundersökningen definieras som positiv respektive negativ påverkan på rapporteringsgraden enligt följande:

Positiv inverkan på rapporteringsgraden: *Instämmer i hög grad* samt *instämmer helt*.
Negativ inverkan på rapporteringsgraden: *Instämmer inte alls* samt *instämmer i låg grad*.

Då det inte är möjligt att avgöra om svarsalternativet *instämmer delvis* betyder delvis negativt eller delvis positivt, alternativ en neutral åsikt, tas denna svarskategori inte med i bedömningen. Däremot kan en betydande andel som svarat *delvis* på en fråga indikera att osäkerheten hos de svarande myndigheterna är stor, vilket i sig kan vara en intressant observation.

Nedan ges en närmare beskrivning av respektive område samt en fördjupning av vad som bedöms vara positiv respektive negativ inverkan på rapporteringsgraden för varje kategori.

3.1.1 Interna rutiner

För att rapportering av allvarliga IT-incidenter ska kunna ske bedömer studieförfattarna att det är en grundläggande förutsättning att myndigheter har interna rutiner för detta ändamål. Definitionen av interna rutiner hämtas från föreskriften MSBFS 2016:1 om statliga myndigheters informationssäkerhet (MSB, 2016b). Enligt föreskriften ska myndigheter ha rutiner för att:

- identifiera
- bedöma
- hantera
- dokumentera
- rapportera inträffade incidenter.[7]

[7] MSBFS 2016:1 s.3.

I studien har vi utgått från att det är positivt för rapporteringsgraden ju större andel myndigheter som uppger att de har interna rutiner enligt ovan. Därtill bedöms effekten på rapporteringsfrekvensen av respektive rutin vara beroende av föregående rutin i ordningen. Med det menas att om en myndighet exempelvis uppger sig ha bra rutiner för att bedöma IT-incidenter, men betydligt sämre rutiner för att identifiera dem blir effekten på rapporteringsgraden inte bättre än rutinen för att identifiera IT-incidenten.

3.1.2 Interna förutsättningar och förankring

Det räcker inte med att endast ha interna rutiner på plats för att rapporteringen ska komma till stånd. För att teori ska kunna översättas i praktik bedömer studieförfattarna att det är nödvändigt att arbetet har givits interna förutsättningar som möjliggör rapporteringen samt att det finns en förankring för uppgiften. Interna förutsättningar och förankring definieras i analysramverket som att:

- det har tillhandahållits information till myndighetens medarbetare om krav på myndigheten att rapportera IT-incidenter till MSB
- det finns en utpekad ansvarig för hanteringen av IT-incidentrapporteringen till MSB
- det finns resurser för att hantera rapporteringen av IT-incidenter till MSB
- det är uttalat från ledningsnivå att det är viktigt att IT-incidenter rapporteras till MSB
- det finns inarbetade rutiner för överföring av sekretessbelagd information mellan myndigheter.[8]

Till de interna förutsättningarna hör således att medarbetare har tillhandahållits information om MSBFS 2016:2 (MSB, 2016c) och dess innebörd. Om så inte har skett undergrävs möjligheten att bidra till att IT-incidenter rapporteras. Vidare ska myndigheten ha registrerat en ansvarig person för att sköta rapporteringen. Risken bedöms annars vara överhängande att uppgiften hamnar mellan stolarna.

Studieförfattarna bedömer även att det är en basal förutsättning att det finns avsatta resurser för att hantera IT-incidentrapporteringen. Om IT-incidentrapportering ska konkurrera med redan befintliga arbetsuppgifter om tillgängliga resurser finns en risk att IT-incidentrapportering får stå tillbaka i konkurrens med andra uppgifter.

En frågas tyngd i en organisation bedöms i studien även vara behjälpt av ett uttalat stöd från ledningsnivå. Om IT-incidentrapporteringen inte har ett uttalat

[8] Detta påstående ligger under *Genomförande* i enkäten men har sedan flyttats för att bättre passa in i analysramverket.

stöd från ledningen bedöms det vara mindre sannolikt att rapporteringen sker i önskvärd omfattning. Slutligen behöver det finnas inarbetade rutiner för överföring av sekretessbelagd information mellan myndigheter i de fall en IT-incident inte bedöms kunna rapporteras enligt ett öppet förfarande.

3.1.3 Genomförande

Genomförande preciseras i analysramverket utifrån följande fem aspekter, nämligen:

- hur enkelt myndigheterna bedömer att det är att avgöra vad som utgör en allvarlig IT-incident som ska rapporteras till MSB
- hur enkelt myndigheterna bedömer att det är att avgöra när en IT-incident ska polisanmälas
- hur enkelt myndigheterna bedömer att det är att avgöra om uppgifter rörande en IT-incident omfattas av sekretess
- hur enkelt myndigheterna bedömer att det är att fylla i MSB:s formulär för IT-incidentrapportering
- om det stödmaterial som erbjuds från MSB och CERT-SE bedöms vara tillräckligt för att myndigheten ska kunna uppfylla kravet på rapportering av IT-incidenter.

Valet av ovanstående aspekter motiveras av studieförfattarna med att de personer som genomför själva IT-incidentrapporteringen behöver en ha grundläggande förmåga att genomföra rapportering i enlighet med MSBFS 2016:2 (MSB, 2016c). Däri framgår att det är respektive myndighet som själv ska bedöma huruvida en IT-incident är allvarlig och om den ska polisanmälas. Det blir därför centralt att ha kunskapen för att genomföra detta. IT-incidentrapporteringen omgärdas även av sekretess i vissa delar. Därför måste ansvariga för IT-incidentrapporteringen ha grundläggande kunskap att avgöra när uppgifter omfattas av sekretess. Det är slutligen nödvändigt att kunna fylla i MSB:s formulär för IT-incidentrapportering.

Det bedöms även vara intressant att i analysramverket fånga upp om det uppfattas finnas tillräckligt med stödmaterial på CERT-SE för att kunna genomföra punkt a-d i listan ovan.

3.1.4 Upplevd nytta

Det fjärde området som studieförfattarna bedömer vara grundläggande för att IT-incidentrapportering ska ske är motivation och drivkraft. I rapportens analysramverk översätts detta till myndigheters uppfattade nytta med IT-incidentrapporteringen.

Upplevd nytta fångas i analysramverket upp av följande påståenden:

På myndigheten upplevs nyttan med myndigheternas rapportering av IT-incidenter till MSB vara att:

- andra myndigheter som riskerar att drabbas av motsvarande IT-incident kan varnas
- bli förvarnad om inträffade IT-incidenter hos andra myndigheter
- ge underlag till MSB:s lägesbild
- handla i enlighet med myndighetens rapporteringsskyldighet
- bidra till att öka svenska myndigheters IT-säkerhetsnivå
- öka medvetenheten internt inom myndigheten om IT-incidenter.

Utöver att ta ställning till ovanstående kategorier gavs även myndigheterna möjlighet att i fritext ange övriga nyttor i enkäten.

3.1.5 Hypotetiska scenarier

Den sista beståndsdelen i analysramverket är två hypotetiska scenarier. Det första scenariot är att en allvarlig IT-incident har inträffat på myndigheten och det andra scenariot är att en IT-incident med ursprung i en brottslig gärning inträffat på myndigheten. Till respektive scenario ges ett antal påståenden om möjliga orsaker till att rapportering av IT-incidenten till MSB respektive anmälan till Polisen inte sker. Enkätrespondenterna uppmanas ta ställning till i vilken grad de instämmer att dessa orsaker skulle kunna vara en anledning till utebliven rapportering.

Enkätens påståenden gällande rapportering till MSB och anmälan till Polisen listas nedan. De tre påståendena som är markerade med asterisk (*) gäller endast för det första scenariot som rör rapportering till MSB.

1. Själva rapporteringsförfarandet att fylla i och mejla incidentrapportmallen till CERT-SE är krångligt.*
2. Att rapportera/anmäla IT-incidenter till MSB/Polisen medför merarbete för myndigheten.
3. Hög arbetsbelastning på myndigheten vid tillfället för IT-incidenten.
4. Myndigheten får inte tillräcklig återkoppling på IT-incidenter som rapporteras till MSB.*
5. Att rapportera/anmäla IT-incidenter till MSB/Polisen är inte en prioriterad uppgift på myndigheten.
6. Myndigheten upplever inte någon nytta med att rapportera/anmäla IT-incidenten till MSB/Polisen.

7. Myndigheten känner sig inte trygg i att sekretessbelagd information lämnar myndighetens kontroll.*
8. Att rapportera/anmäla IT-incidenter till MSB/Polisen kan medföra oönskad exponering av myndighetens IT-relaterade problem.
9. Myndigheten saknar rutiner för att rapportera/polisanmäla IT-incidenter.
10. Myndighetens rutiner för att rapportera/polisanmäla IT-incidenter är inte inarbetade.
11. IT-incidenten bedöms initialt inte vara tillräckligt allvarlig för att behöva rapporteras/anmälas till MSB/Polisen.
12. Nödvändig kompetens för att rapportera/polisanmäla IT-incidenter saknas på grund av omsättning av nyckelpersoner.

Påståendena syftar till att ge myndigheterna en möjlighet att svara på tänkbara anledningar till att rapportering till MSB eller polisanmälan inte sker, utan att avslöja information om någon inträffad IT-incident som kan omfattas av sekretess. De hypotetiska scenarierna kan ge en kompletterande och nyanserad bild av vilka orsaker myndigheterna uppfattar kan ligga bakom utebliven rapportering.

3.2 Mer om enkäten och dess respondenter

Enkäten skickades ut till alla rapporteringsskyldiga myndigheter. Totalt sett var det 249 myndigheter. Svarsfrekvensen låg på drygt 70 procent.

För att möjliggöra för rapporteringsskyldiga myndigheter att svara på enkäten på ett så fritt sätt som möjligt besvarades den anonymt. Det i sin tur medförde att enkäten skickades ut i pappersformat då ett elektroniskt förfarande inte kunde garantera anonymitet. Enkäten skrevs ut på papper och skickades till respektive myndighets registratur med ett följebrev som informerade om enkätens tilltänkta mottagare (se Bilaga A). Adresser till rapporteringsskyldiga myndigheter hämtades från Statistiska centralbyråns myndighetsregister (SCB, u.å.).

I enkätens inledande frågor uppmanas respondenterna att välja mellan fem olika storlekskategorier baserat på hur många anställda respektive myndighet har.[9] Valet av storleksspann på kategorierna baserades på hur storleksfördelningen ser ut bland myndigheter, och syftar till att få en så jämn fördelning av potentiella svar i varje kategori som möjligt. Bevakningsansvariga myndigheter[10]

[9] Valda storlekskategorier utifrån antal anställda: 0-25, 26-100, 101-300, 301-1000, >1000 samt bevakningsansvariga myndigheter.

[10] De bevakningsansvariga myndigheter som omfattas av rapporteringsskyldigheten spänner storleksmässigt mellan ca 50 och drygt 10 000 anställda.

uppmanades att inte fylla i frågan om antalet anställda för att minska sannolikheten att kunna identifiera vilken bevakningsansvarig myndighet som hade besvarat enkäten.

Respondenterna gavs dessutom möjlighet att besvara följande två frågor med fritext:

- Anser du att MSB bör förändra något avseende IT-incidentrapporteringen för att myndigheten ska börja rapportera eller öka rapporteringen av IT-incidenter?
- Har du några ytterligare synpunkter eller kommentarer som inte fångas upp av enkäten?

Efter att enkäten skickats ut blev studieförfattarna uppmärksammade på att nio myndigheter felaktigt var med på utskickslistan. En myndighet hade inkluderats av misstag, resterande åtta bedömdes i samråd med MSB vara undantagna rapporteringsskyldigheten då de har Regeringskansliet som värdmyndighet[11]. I sammanhanget bör nämnas att MSB hittills har inkluderat de åtta myndigheterna i sin lista över rapporteringsskyldiga myndigheter, vilket inneburit att myndigheterna finns representerade i den statistik över rapporteringsgraden som MSB presenterar i sina årsrapporter.

Av de nio myndigheter som felaktigt har fått enkäten skickad till sig har fyra myndigheter varit i kontakt med FOI, och det har därför kunnat säkerställas att dessa inte har svarat på enkäten. Det innebär att bland de enkätsvar som inkom till FOI kan fem vara från myndigheter som egentligen inte är att betrakta som rapporteringsskyldiga. Samtliga av de myndigheter som berörs är små myndigheter och faller inom kategorin 0-25 anställda.

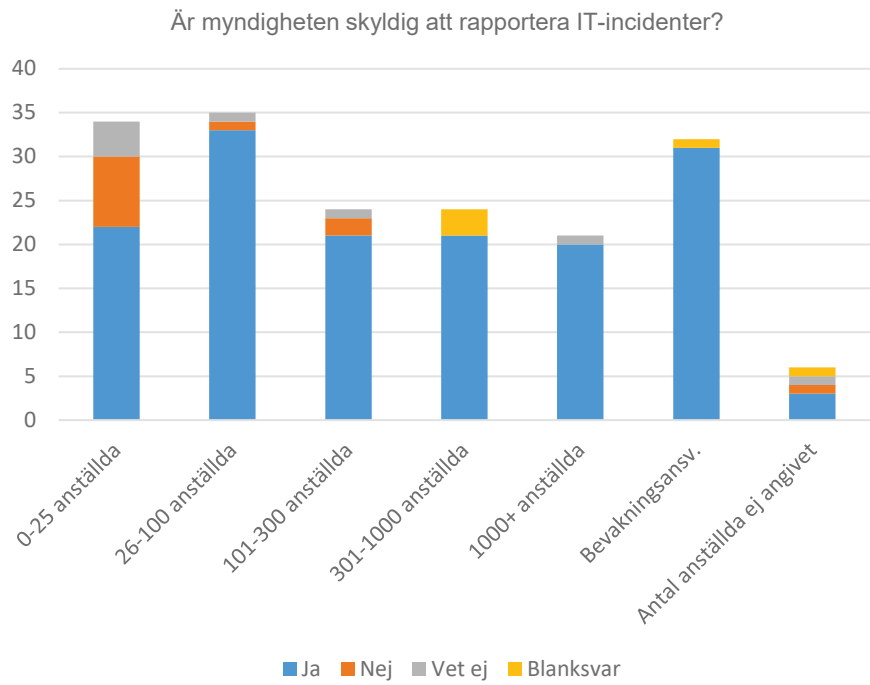
I en enkätundersökning får man räkna med att vissa enkäter inte är fullständigt eller korrekt ifyllda. I denna enkätundersökning har ofullständiga svar hanterats genom att utesluta svaret på de delfrågor där blanka svar har förekommit.

[11] Regeringskansliet är undantaget från rapporteringsskyldigheten.

4 Resultat

I detta kapitel presenteras ett bearbetat resultat av enkätundersökningen utifrån analysramverket. Enkätresultatet i sin helhet återfinns i de två bilagorna B och C.

Av 249 utskickade enkäter[12] inkom 176 svar till FOI, vilket ger en svarsfrekvens på 70,7 procent. Figur 3 illustrerar hur fördelningen ser ut gällande vilka myndigheter som uppger att de är rapporteringsskyldiga enligt MSBFS 2016:2 (MSB, 2016c). Av de 176 inkomna enkätsvaren uppger 12 myndigheter att de inte är rapporteringsskyldiga. Figuren visar även att svarsfrekvensen för respektive storlekskategori är relativt jämn med 21 till 35 svarande per kategori.



Figur 3: Diagrammet visar myndigheternas svar på frågan om de är rapporteringsskyldiga enligt MSBFS 2016:2, med enkätsvaren grupperat efter myndighetskategori.

[12] Siffran är korrigerad för felaktiga samt kompletterade enkätutskick, se Metodkapitlet.

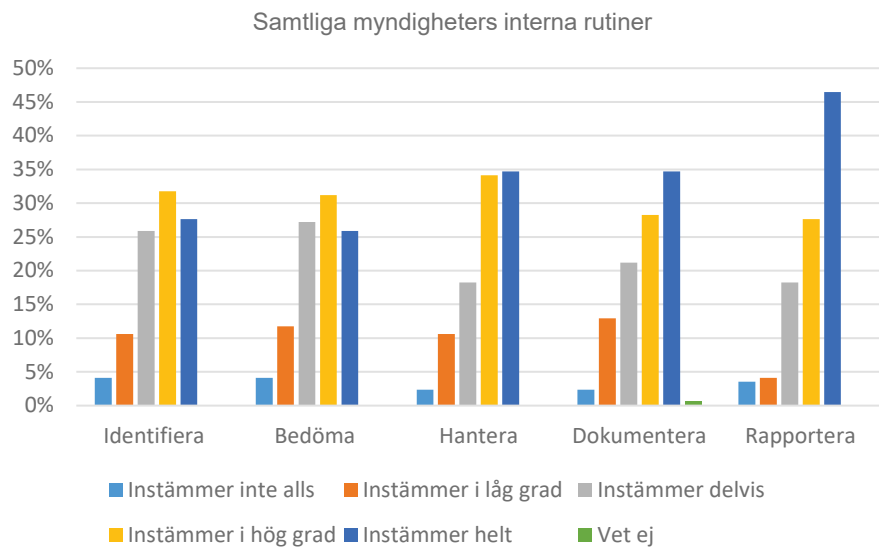
4.1 Interna rutiner

I detta avsnitt presenteras enkätresultaten med avseende på vilka interna rutiner som myndigheter uppger att de har.

Interna rutiner definieras enligt analysramverket som rutiner för att:

- identifiera
- bedöma
- hantera
- dokumentera
- rapportera IT-incidenter.

Som framkommer av Figur 4 visar enkätsvaren för samtliga myndigheter att den rutin som flest myndigheter instämmer med att de har *i hög grad* eller *helt* är för att rapportera IT-incidenter, medan de rutiner som minst antal myndigheter instämmer med att de har *i hög grad* eller *helt* är för att identifiera samt bedöma IT-incidenter.



Figur 4: Fördelningen av hur väl myndigheterna instämmer med att de har interna rutiner relaterat till IT-incidentrapportering.

Ur enkätresultaten framkommer att andelen myndigheter som *instämmer helt* eller *i hög grad* samt instämmer *i låg grad* eller *inte alls* fördelas över de interna rutinerna enligt Tabell 1. I tabellen kan ses att myndigheter i lägre utsträckning har rutiner för att identifiera och bedöma IT-incidenter än för att rapportera dem.

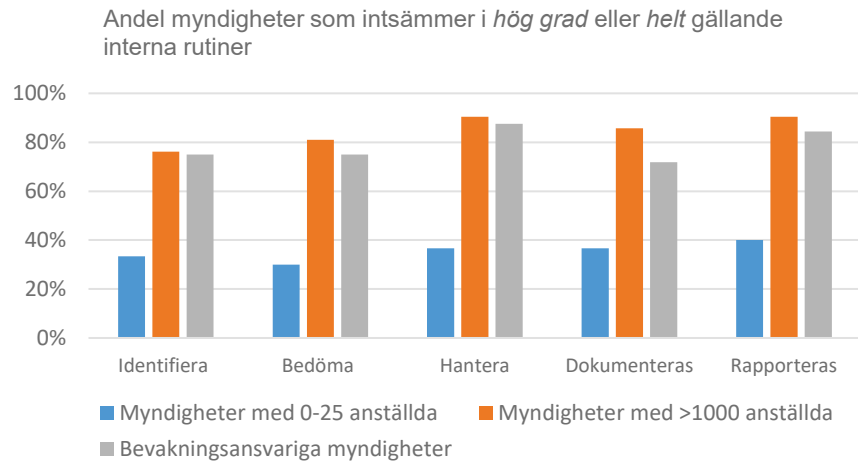
Tabell 1: Andel av samtliga myndigheter som instämmer *i hög grad* eller *helt,* samt instämmer *i låg grad* eller *inte alls* till att de har respektive rutin.

	Identifiera	Bedöma	Hantera	Dokumentera	Rapportera
Instämmer i *hög grad* eller *helt*	60 %	57 %	69 %	63 %	74 %
Instämmer *i låg grad* eller *inte alls*	15 %	16 %	13 %	15 %	8 %

En analys av enkätresultatet visar att 46 procent av alla myndigheter svarat att de instämmer *helt* eller *i hög grad* för samtliga fem rutiner. Det betyder att det är knappt hälften av myndigheterna som genomgående har rutiner på plats för att identifiera, bedöma, hantera, dokumentera och rapportera IT-incidenter. Om utgångspunkten är att alla rapporteringsskyldiga myndigheter förväntas ha samtliga rutiner för att kunna uppfylla sin skyldighet att rapportera in allvarliga IT-incidenter till MSB är 46 procent en relativt låg siffra. Det faktum att mer än hälften av myndigheterna har en eller flera rutiner som brister utgör en sannolik källa till negativ inverkan på rapporteringsfrekvensen.

När resultatet studeras för respektive myndighetskategori visar enkätsvaren tydligt att det genomgående är bevakningsansvariga myndigheter samt myndigheter med fler än 1000 anställda som har störst andel med samtliga rutiner på plats. Omvänt visar enkätresultaten att det är de minsta myndigheterna med 0-25 anställda som har minst andel myndigheter med interna rutiner på plats.

Skillnaden i rutiner mellan de minsta och största samt bevakningsansvariga myndigheter framkommer tydligt i Figur 5. Förutsättningarna för små myndigheters rapporteringsförfarande är med andra ord märkbart sämre än för de största samt bevakningsansvariga myndigheterna.



Figur 5: Fördelningen av myndigheter som instämmer *i hög grad* eller instämmer *helt* med att de har respektive rutin, grupperat efter myndighetskategorierna: myndigheter med 0-25 anställda, fler än 1000 anställda och bevakningsansvariga myndigheter.

4.2 Interna förutsättningar och förankring

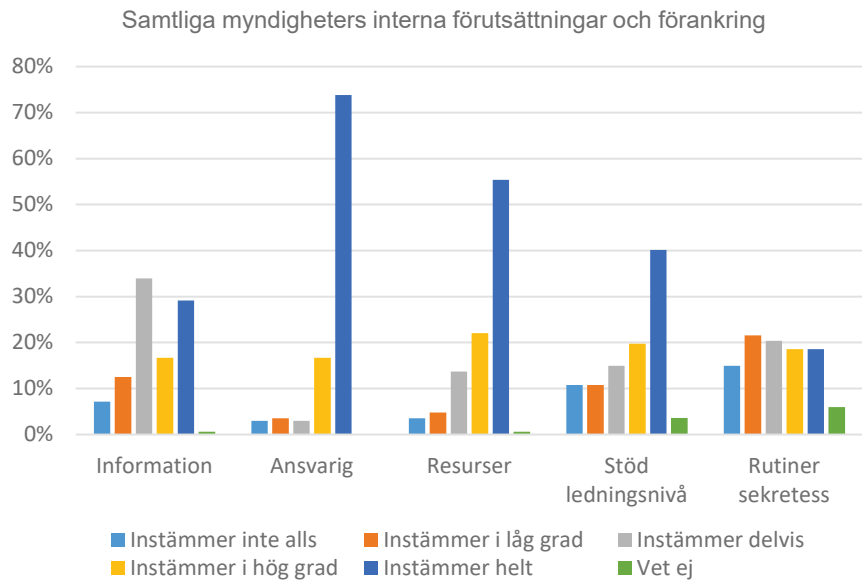
Enligt analysramverket studeras myndigheternas interna förutsättningar och förankring enligt följande parametrar:

- att det har tillhandahållits information till myndighetens medarbetare om krav på myndigheten att rapportera IT-incidenter till MSB
- att det finns en utpekad ansvarig för hanteringen av IT-incidentrapporteringen till MSB
- att det finns resurser för att hantera rapporteringen av IT-incidenter till MSB
- att det är uttalat från ledningsnivå att det är viktigt att IT-incidenter rapporteras till MSB
- att det finns inarbetade rutiner för överföring av sekretessbelagd information mellan myndigheter.

Som framkommer av Figur 6 visar resultatet för samtliga myndigheter att en relativt stor andel uppger att de instämmer *helt* eller *i hög grad* i påståendena om att det finns en utpekad ansvarig samt resurser för att hantera rapporteringen av IT-incidenter till MSB. För övriga påståenden, att information har tillhandahållits medarbetare, att det finns ett uttalat stöd från ledningen samt förekomsten av

inarbetade rutiner för överföring av sekretessbelagd information mellan myndigheter, är motsvarande andelar mindre.

Resultatet för respektive myndighetskategori överensstämmer på det stora hela med resultatet för samtliga myndigheter.



Figur 6: Fördelning av hur väl myndigheterna instämmer med att de har interna förutsättningar och förankring för IT-incidentrapportering.

Enkätresultatet för myndigheternas interna förutsättningar och förankring ger således en tudelad bild. Å ena sidan är det en styrka att det i hög utsträckning finns en utpekad ansvarig samt att resurser upplevs finnas, och är något som torde ha en positiv inverkan på rapporteringsfrekvensen. Men å andra sidan är det svaga stödet för informationsspridning till medarbetare något som sannolikt undergräver rapporteringsmöjligheten då det är medarbetarna som till del upptäcker och delvis orsakar IT-incidenter.

Här kan det vara värt att stanna upp och ställa sig frågan vilka medarbetare som är i behov av informationen angående den obligatoriska IT-incidentrapporteringen till MSB för att rapporteringen ska fungera som det är tänkt. Varje anställd vid en myndighet är en potentiell måltavla för angrepp som exempelvis nätfiske, och kan även vara orsaken till IT-incidenter genom handhavandefel. För andra kategorier av IT-incidenter där enskilda medarbetare

inte nödvändigtvis är måltavla, som exempelvis störning i driftmiljön eller hindrad tillgång till information, är det inte givet att information till varje enskild medarbetare om IT-incidentrapportering har någon större inverkan på rapporteringsfrekvensen.

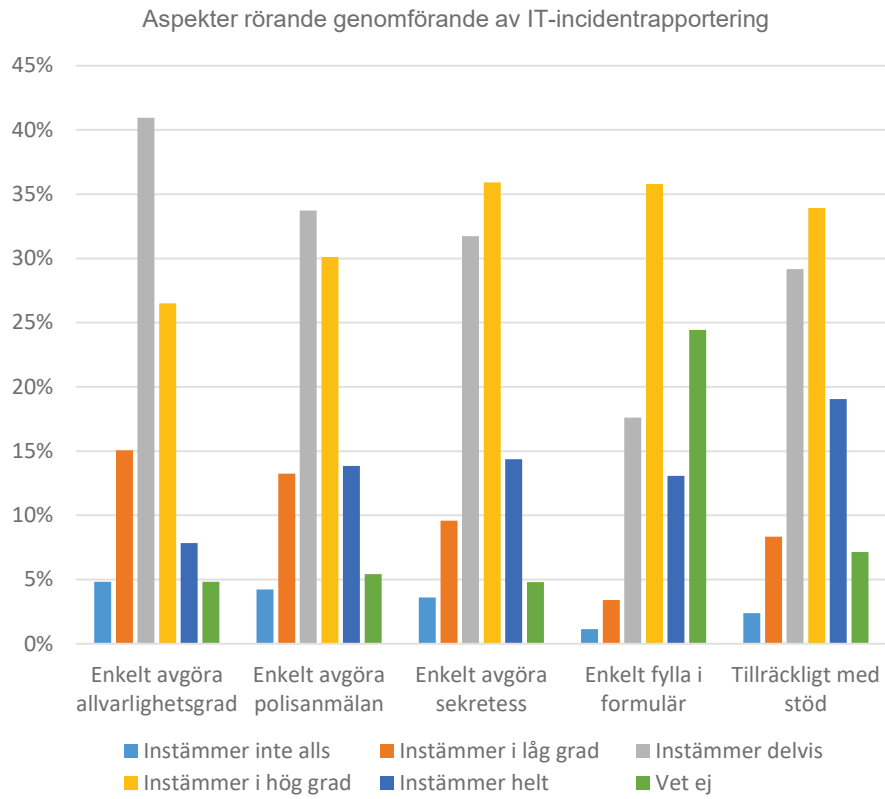
Vad gäller rutiner för överföring av sekretessbelagd information mellan myndigheter är även denna parameter ett tänkbart hinder för rapporteringen. Det kan sannolikt vara utmanande att hinna rapportera in IT-incidenter inom 24 timmar om dessa rutiner inte finns på plats.

4.3 Genomförande

Som beskrivs i rapportens metodavsnitt väljer studieförfattarna att fånga aspekter som rör att genomföra en rapportering i enlighet med direktiv 2016:2 utifrån följande:

- hur enkelt myndigheterna bedömer att det är att avgöra vad som utgör en allvarlig IT-incident som ska rapporteras (detta eftersom det i MSBFS 2016:2 framgår att det är respektive myndighet som själv själva ska bedöma huruvida en IT-incident är allvarlig eller inte)
- hur enkelt myndigheterna bedömer att det är att avgöra om en IT-incident ska polisanmälas (likt föregående punkt är det myndigheten själv som ska göra denna bedömning)
- hur enkelt myndigheterna bedömer att det är att avgöra om uppgifter rörande en IT-incident omfattas av sekretess (detta eftersom uppgifter i IT-incidentrapporteringen kan omfattas av sekretess och därmed behöver överföras till MSB på ett därför lämpligt sätt)
- hur enkelt myndigheterna bedömer att det är att fylla i MSB:s formulär för IT-incidentrapportering (detta eftersom det för att rapportering ska kunna ske är nödvändigt att exempelvis förstå vilken information som efterfrågas i formuläret)
- om det stödmaterial som erbjuds från MSB och CERT-SE bedöms vara tillräckligt (detta då det är en förutsättning att MSB och CERT-SE tillhandahåller tillräckligt med vägledning i form av instruktioner, exempel och stödmaterial för att myndigheterna ska kunna rapportera IT-incidenter i enlighet med MSBFS 2016:2).

I detta avsnitt analyseras resultaten för enkätens frågor rörande ovanstående punkter. I Figur 7 ges en övergripande bild av hur myndigheterna har svarat.



Figur 7: Fördelning av hur väl myndigheterna instämmer med de fem aspekterna rörande genomförande av IT-incidentrapportering.

Huruvida det är enkelt att avgöra vad som är en allvarlig IT-incident som ska rapporteras och vad som inte är det verkar det råda delade meningar om. Även om det är fler myndigheter som anser att det är relativt enkelt (34 procent) är det samtidigt 20 procent som svarat att de *inte alls* eller *i låg grad* instämmer i detta påstående. De minsta myndigheterna utmärker sig i sammanhanget som de som verkar uppleva de största utmaningarna i att avgöra allvarlighetsgraden.[13] Enkätresultaten visar i övrigt inget samband mellan myndighetens storlek och hur enkelt myndigheterna uppger att det är att bedöma incidenterna.

[13] 34 procent av myndigheterna i storlekskategorin 0-25 anställda instämmer inte alls eller i låg grad i påståendet att det är enkelt att avgöra om en IT-incident är rapporteringsskyldig eller ej.

Vad gäller polisanmälan så visar enkätresultaten att myndigheterna överlag anser att det är något enklare att avgöra om en IT-incident ska polisanmälas än att avgöra om den är av sådan karaktär att den ska rapporteras till MSB.[14] Likt för förmågan att avgöra om en IT-incident ska rapporteras till MSB utmärker sig de minsta myndigheterna som de som i minst grad instämmer. Det finns dock inget i enkätresultaten som visar på att det finns något samband mellan myndighetens storlek och hur de svarat på denna enkätfråga.

Gällande sekretessfrågan visar resultaten att det är markant fler myndigheter som upplever att det är relativt enkelt att avgöra om uppgifter rörande en inträffad IT-incident omfattas av sekretess än de som inte anser det (50 procent instämmer *helt* eller *i hög grad*, 13 procent instämmer *inte alls* eller *i låg grad*). Framför allt är det de mindre myndigheterna som inte instämmer (28 procent i kategorin 0-25 anställda, och 18 procent i kategorin 26-100 anställda).

Det är också markant fler myndigheter som instämmer i att det är enkelt att fylla i MSB:s formulär för IT-incidentrapportering än de som inte gör det (49 procent instämmer *helt* eller *i hög grad*, 5 procent instämmer *inte alls* eller *i låg grad*). Det finns dock stora skillnader mellan hur de olika myndighetskategorierna svarat. Medan minst 70 procent av myndigheter med fler än 300 anställda instämmer *i hög grad* eller *helt* i påståendet, är motsvarande andel bara 14 procent för myndigheter med 0-25 anställda.

Slutligen, som framgår av enkätresultaten svarar fler än hälften av myndigheterna att de *helt* eller *i hög grad* instämmer i påståendet om att det finns tillräckligt med stödmaterial rörande IT-incidentrapporteringen. I grova drag kan man således beskriva myndigheternas inställning till det befintliga utbudet som att hälften av dem anser att det är någorlunda tillfredsställande, medan hälften anser att det finns brister av varierande grad. Värt att notera är att det finns påfallande skillnader mellan olika kategorier av myndigheter. 71 procent av de bevakningsansvariga myndigheterna instämmer *helt* eller *i hög grad* i påståendet, att jämföra med 24 procent av de allra minsta myndigheterna (0-25 anställda).

4.3.1 Kommentarer på resultatet

För alla frågor som behandlas i detta avsnitt utmärker sig de allra minsta myndigheterna (0-25 anställda) med att en betydande andel av dem besvarat enkätens frågor med alternativet *Vet ej*. Det kan tolkas som ett tecken på att myndigheterna hittills inte har rapporterat eller polisanmält några allvarliga IT-incidenter, alternativt att den som fyllt i enkäten inte har kännedom om tidigare

[14] 44 procent av myndigheterna anser att de *helt* eller *i hög grad* håller med om påståendet att det är enkelt att avgöra när en IT-incident ska polisanmälas. Motsvarande 17 procent uppger att de *inte alls* eller *i låg grad* instämmer.

inrapporterade och polisanmälda incidenter och därmed inte vet hur enkelt det är att bedöma exempelvis allvarlighetsgrad och sekretess. Oavsett anledning är andelen som har svarat *Vet ej* betydligt högre än för någon av de andra myndighetskategorierna.

4.4 Upplevd nytta

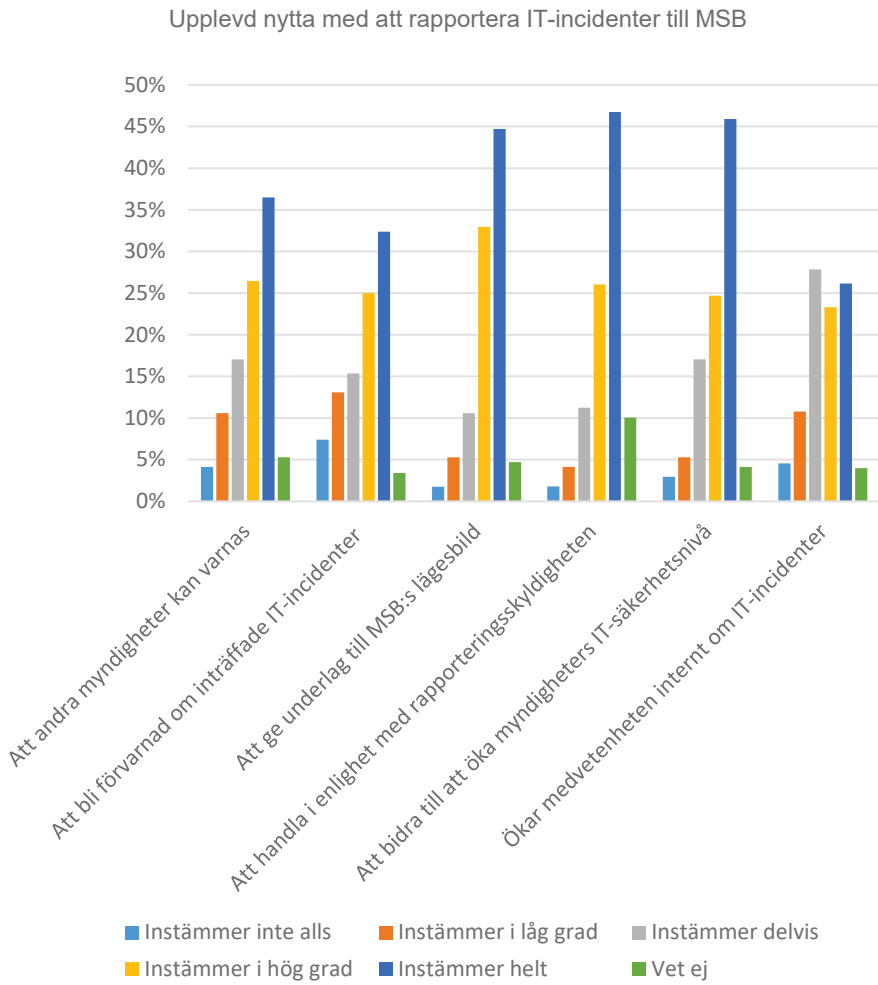
Myndigheternas upplevda nytta med rapportering av IT-incidenter till MSB skulle kunna påverka deras motivation och drivkraft att rapportera inträffade IT-incidenter. Eftersom myndigheterna själva avgör om en IT-incident är tillräckligt allvarlig för att rapporteras skulle en bristande upplevd nytta kunna ha en negativ inverkan på motivationen att inom organisationen prioritera rapportering.

Som kan ses i Figur 8 som sammanfattar resultaten för enkätens frågor om upplevd nytta med rapporteringen, anger myndigheterna överlag en (hög) nytta med IT-incidentrapporteringen. Av 176 enkätsvar är det endast fyra myndigheter, två procent, som konsekvent angett att de *inte alls* eller *i låg grad* instämmer med att IT-incidentrapporteringen skulle bidra till någon av de i enkäten angivna nyttoaspekterna. Ingen av dessa fyra myndigheter har heller i enkätens relaterade fritextfråga angivit någon annan form av nyttoaspekt med rapporteringen. Av samtliga myndigheter angav 157 stycken, det vill säga 89 procent, att de *helt* eller *i hög grad* instämde med minst en av de i enkäten angivna nyttoaspekterna.

Den nyttoaspekt som minst antal myndigheter håller med om är att hela rapporteringssystemet skulle bidra till att kunna bli förvarnad om inträffade IT-incidenter hos andra myndigheter. Studieförfattarnas kommentar till det är att myndigheterna kanske inte upplever att den information som ges från MSB om inträffade IT-incidenter är tillräckligt detaljerad för att kunna vara till nytta i organisationen, alternativt att informationen om inträffade IT-incidenter kommer för sent.

När myndigheterna i fritextsvar fick möjlighet att uttrycka nytta, utöver de i enkäten föreslagna aspekterna som visas i Figur 8, framhöll några myndigheter att de råd och det stöd som tillhandahålls från MSB upplevdes vara till nytta. En myndighet menade att arbetet med att rapportera IT-incidenterna ger en samlad historik av inträffade IT-incidenter, vilket skapar ett bra underlag för myndighetens egen uppföljning och för att förbättra IT-säkerheten.

I fritextsvaren lyfter även ett tiotal myndigheter fram att skyldigheten att rapportera IT-incidenter till MSB aktualiserar IT-säkerhetsarbetet ytterligare och visar på vikten med detta arbete ända upp på ledningsnivå. Genom skyldigheten att rapportera påtalas vikten av att ha en bra beredskap för att hantera IT-incidenter, vilket resulterar i både tid och stöd från myndighetens ledning för att åtgärda eventuella brister som identifieras.



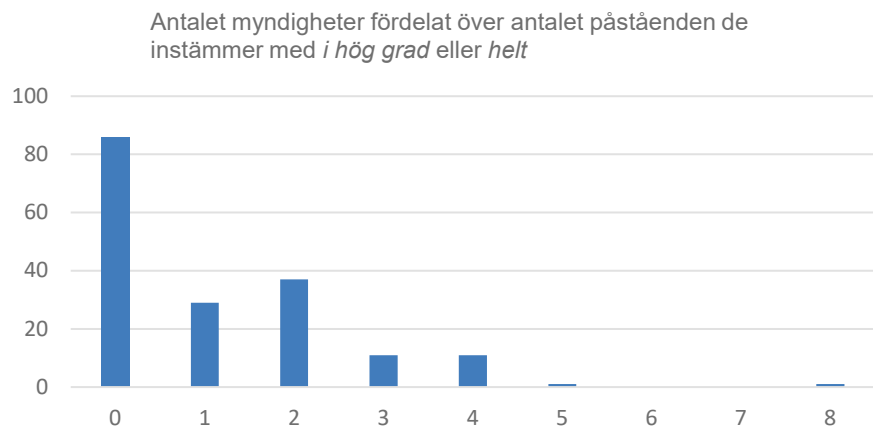
Figur 8: Fördelning av hur väl myndigheterna instämmer med att de upplever nytta med IT-incidentrapporteringen.

4.5 Anledningar att inte rapportera

I syfte att fånga upp möjliga anledningar till att myndigheter inte rapporterar IT-incidenter till MSB innehöll enkäten ett hypotetiskt scenario som beskriver att det vid en myndighet inträffat en allvarlig IT-incident men att rapportering av denna uteblivit. Kopplat till scenariot fanns 12 påståenden som beskriver möjliga anledningar till varför rapporteringen uteblivit (se avsnitt 3.1.5). I enkäten fick myndigheterna ta ställning till i vilken utsträckning som de bedömde att respektive påstående kunde utgöra anledningar till att rapportering, ur deras egen myndighets perspektiv, uteblivit i scenariot.

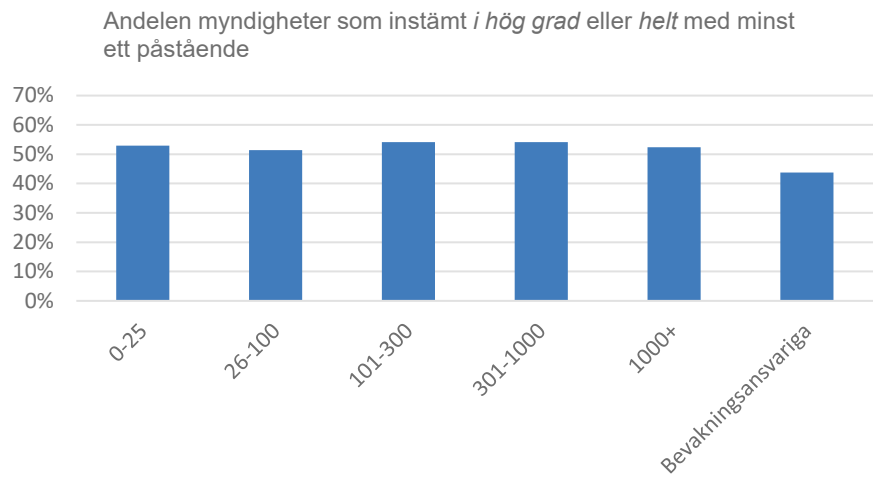
En genomgång av enkätsvaren för de tolv påståendena visar att det generellt är få myndigheter som svarar att de instämmer *i hög grad* eller *helt* med respektive påstående. Det finns med andra ord inte något enskilt påstående som utmärker sig som en huvudsaklig anledning till varför rapportering av IT-incidenter skulle kunna utebli.

Figur 9 visualiserar hur många påståenden som myndigheterna instämde med *i hög grad* eller *helt*. Av totalt 176 myndigheter instämde 90 (dvs. 51 procent) med minst ett av påståendena. Resultaten tyder således på att det kan vara flera olika anledningar som var och en bidrar lite grand till det av MSB upplevda låga antalet rapporteringar av IT-incidenter.



Figur 9: X-axeln visar antalet påståenden som en myndighet har instämt med *i hög grad* eller *helt*. Y-axeln visar antalet myndigheter. Totalt antal svarande myndigheter var 176. Ingen myndighet svarade att de instämde *i hög grad* eller *helt* med fler än åtta påståenden (av de tolv stycken angivna).

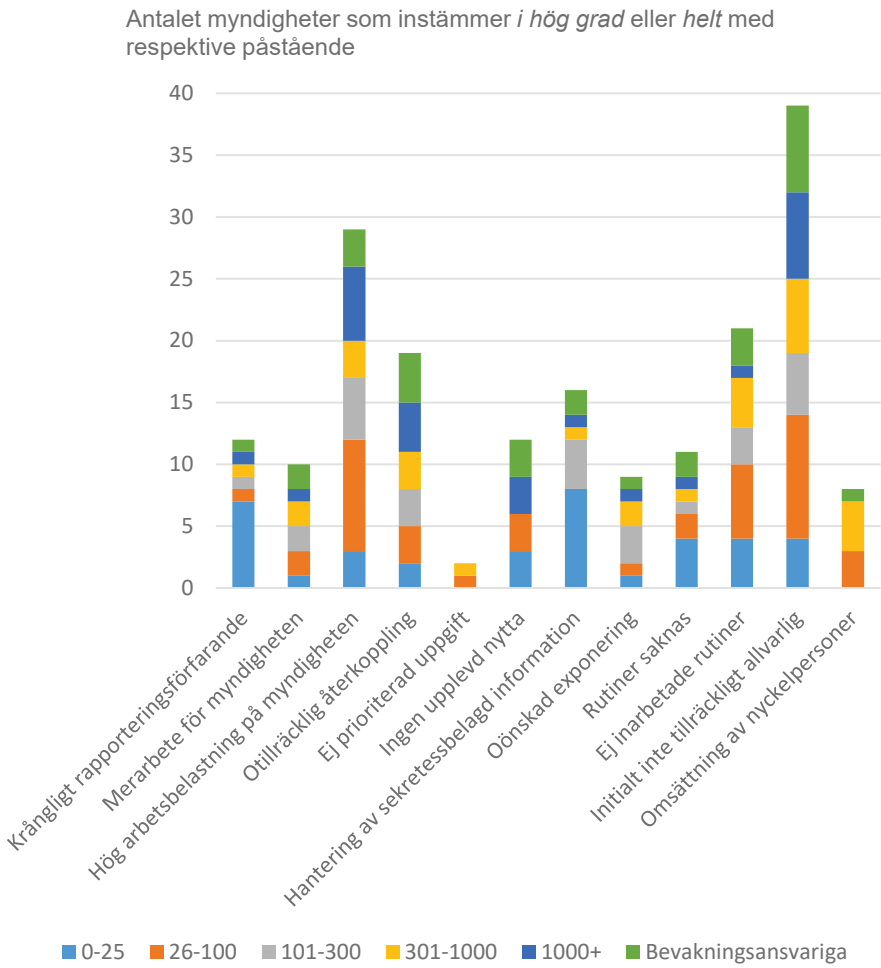
I Figur 10 visas andelen myndigheter per myndighetskategori som instämde *i hög grad* eller *helt* med minst ett av de tolv påståendena. Den fördelning som sågs på övergripande nivå, med 51 procent som instämde positivt, har även en motsvarande fördelning sett till de sex myndighetskategorierna. Det verkar således inte ha någon betydelse hur stor myndigheten är när det kommer till att se möjliga anledningar till att incidentrapportering till MSB kan utebli.



Figur 10: Andelen myndigheter, grupperat utifrån myndighetskategori, som instämmer *i hög grad* eller *helt* med minst ett av de tolv påståendena som utgjorde det hypotetiska scenariot.

För att få en samlad bild av vilka påståenden som myndigheterna instämmer med *i hög grad* eller *helt* har dessa sammanställts i Figur 11. Grafens staplar visar utöver antalet myndigheter som instämmer per påstående även fördelningen mellan de sex myndighetskategorierna. Det framgår även av Figur 11 att det finns en stor spridning mellan vilka möjliga anledningar till att inte rapportera som de olika myndighetskategorierna instämmer med. Det finns alltså inga tydliga tecken på att det skulle finnas någon koppling mellan myndighetskategori och en specifik anledning till att inte rapportera. De tre påståenden som flest myndigheter instämmer med *i hög grad* eller *helt* är:

1. IT-incidenten bedömdes initialt inte vara tillräckligt allvarlig för att behöva rapporteras till MSB
2. hög arbetsbelastning på myndigheten vid tillfället för IT-incidenten
3. myndighetens rutiner för att rapportera IT-incidenter är inte inarbetade.



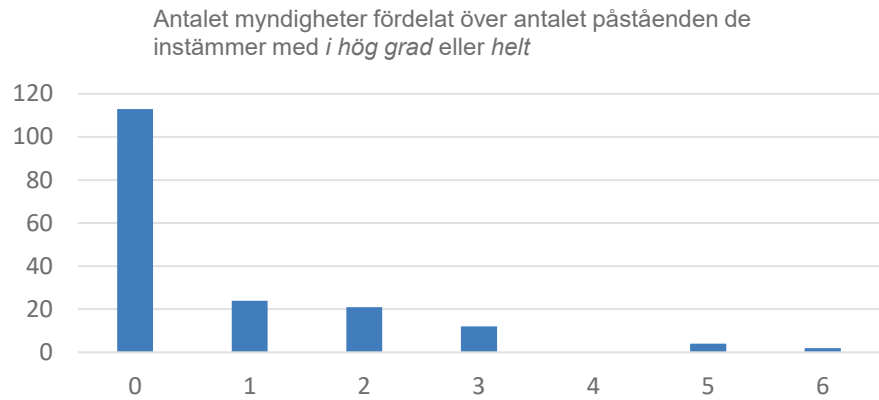
Figur 11: Antalet myndigheter som instämmer *i hög grad* eller *helt* med respektive påstående, grupperat utifrån de tolv påståendena som utgjorde det hypotetiska scenariot.

4.6 Anledningar att inte polisanmäla

I syfte att fånga upp möjliga anledningar till att myndigheter inte polisanmäler allvarliga IT-incidenter med ursprung i en brottslig gärning innehöll enkäten ytterligare ett hypotetiskt scenario där en allvarlig IT-incident har inträffat. Myndigheterna fick svara på i vilken utsträckning som nio olika påståenden

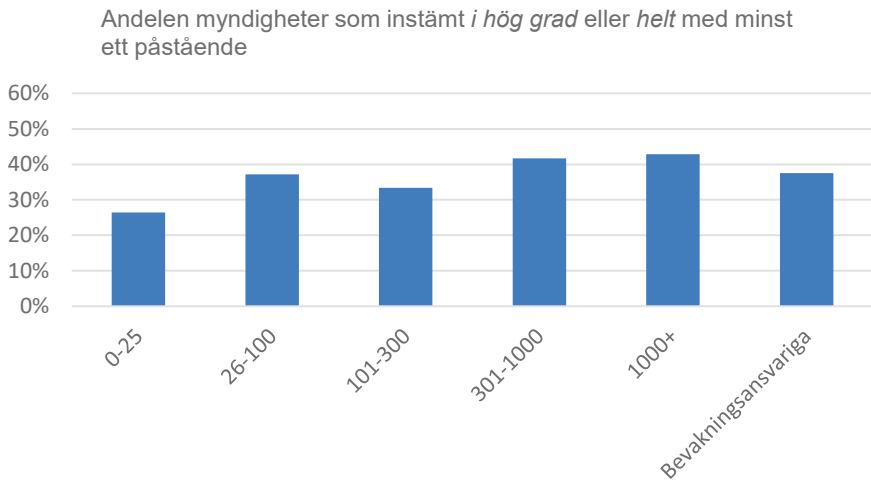
(avsnitt 3.1.5) skulle kunna utgöra möjliga anledningar till att polisanmälan inte görs.

Likt det hypotetiska scenariot med anledningar till att rapportering av IT-incidenter till MSB uteblir (avsnitt 4.5) så saknas det även i detta fall ett enskilt påstående som utmärker sig som en huvudsaklig anledning till varför polisanmälan av allvarliga IT-incidenter inte sker. En analys av hur många påståenden som varje myndighet instämde med *i hög grad* eller *helt* (Figur 12) visar att 36 procent av myndigheterna instämmer med minst ett av dessa påståenden. Det ser således ut som att det kan finnas flera anledningar till att inte polisanmäla en IT-incident som var och en bidrar lite grand till det av MSB upplevt låga antalet polisanmälningar.



Figur 12: X-axeln visar antalet påståenden som en myndighet har instämt med *i hög grad* eller *helt*. Y-axeln visar antalet myndigheter. Totalt antal svarande myndigheter var 176. Ingen myndighet svarade att de instämde *i hög grad* eller *helt* med fler än sex påståenden (av de nio angivna).

De 63 myndigheter som instämmer *i hög grad* eller *helt* med minst ett av de nio påståendena har en jämn fördelning över de olika myndighetskategorierna, vilket visualiseras i Figur 13. Det verkar således inte ha någon betydelse hur stor myndigheten är när det kommer till att se möjliga anledningar till att polisanmälan kan utebli.

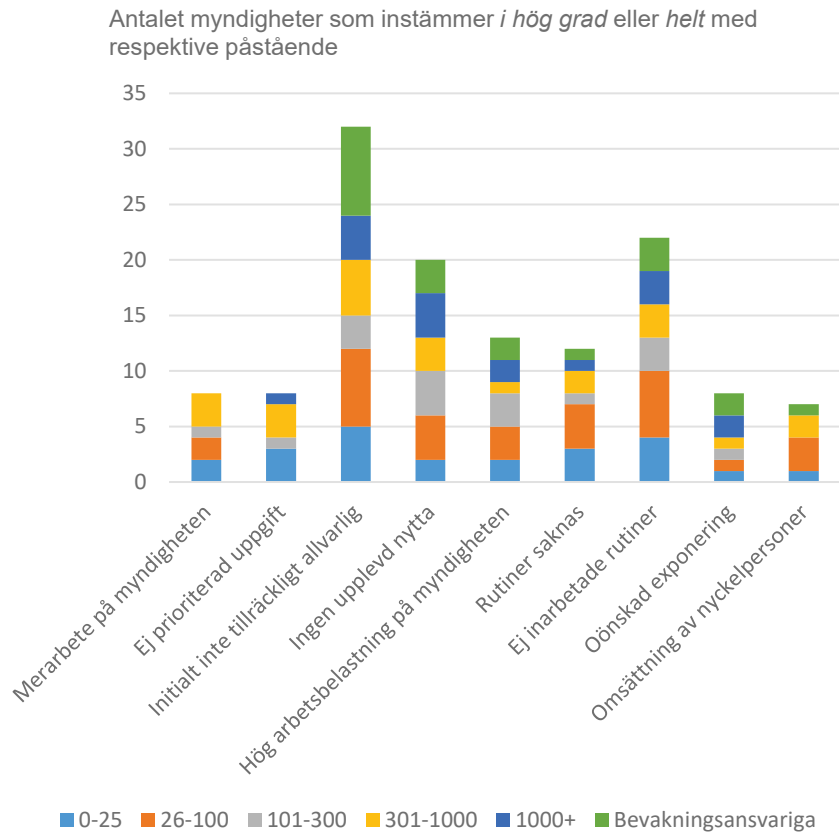


Figur 13: Andelen myndigheter, grupperat utifrån kategori, som instämmer *i hög grad* eller *helt* med minst ett av de nio påståendena som utgjorde det hypotetiska scenariot.

För att få en samlad bild av vilka påståenden som myndigheterna instämmer med *i hög grad* eller *helt* har dessa sammanställts i Figur 14. I figuren går inte bara att utläsa antalet myndigheter som instämmer *i hög grad* eller *helt* med varje påstående, utan även fördelningen mellan de sex myndighetskategorierna. Det ser inte ut att finnas några tydliga samband mellan myndighetens kategori och vilka påståenden som myndigheterna instämmer med.

De tre påståenden som flest myndigheter instämmer med *i hög grad* eller *helt* är:

1. IT-incidenten bedöms initialt inte vara tillräckligt allvarlig för att behöva polisanmälas
2. myndighetens rutiner för att polisanmäla IT-incidenter är inte inarbetade
3. myndigheten upplever ingen nytta med att polisanmäla IT-incidenten.



Figur 14: Antalet myndigheter som instämmer *i hög grad* eller *helt* med respektive påstående, grupperat utifrån de nio påståendena som utgjorde det hypotetiska scenariot.

5 Diskussion

Det avslutande steget i den genomförda studien är att diskutera kring de framkomna resultaten. I avsnitt 5.1 till 5.5 diskuteras möjliga anledningar till att myndigheter inte rapporterar IT-incidenter till MSB, medan avsnitt 5.6 diskuterar möjliga anledningar till att myndigheter inte polisanmäler IT-incidenter med ursprung i brottsliga gärningar.

5.1 Bristande interna rutiner?

För att kunna rapportera allvarliga IT-incidenter till MSB behöver myndigheter ha interna rutiner som möjliggör detta. Sett till samtliga myndigheter är det dock knappt hälften som uppger att de har alla fem studerade rutiner i *hög grad* eller *helt.* Bland de minsta myndigheterna är det endast 35 procent som uppger att de har samtliga rutiner i *hög grad* eller *helt* medan, motsvarande andel hos de största och bevakningsansvariga myndigheterna är ungefär 70 procent. De interna rutinerna brister således i större omfattning hos de minsta myndigheterna, än hos myndigheter med fler än 1000 anställda samt hos bevakningsansvariga myndigheter.

Vidare visar enkätresultatet att en större andel myndigheter uppger att de har rutiner för att rapportera, dokumentera och hantera IT-incidenter än de har för att identifiera och bedöma dem. En tänkbar slutsats är därför att en större andel myndigheter med rutiner för att identifiera och bedöma incidenter skulle möjliggöra att fler allvarliga IT-incidenter blir föremål för rapportering.

Resultatet för det hypotetiska scenariot för utebliven rapportering nyanserar dock frågan om rutiner något. Det förekommer nämligen inte något påtagligt stöd för påståendet om att bristande rutiner kan leda till att rapportering uteblir (Figur 11 i avsnitt 4.5). Det talar för att det finns myndigheter som har bristande rutiner, men som inte själva upplever det som ett hinder för att rapportera IT-incidenter. Det påstående i det hypotetiska scenariot som däremot fick tredje starkast medhåll bland myndigheterna som en möjlig anledning till utebliven rapportering var *ej inarbetade rutiner för att rapportera IT-incidenter*.

Frågan blir då hur de två perspektiven, rutiners befintlighet respektive rutiners inarbetning, påverkar att rapportering inte sker. Ett sammanvägt svar på frågan kan vara att för de myndigheter som uppger att de har rutiner, om än i varierande utsträckning, är det avsaknaden av erfarenhet att använda dem som påverkar rapporteringsgraden negativt. För de myndigheter som däremot saknar rutiner helt eller i stor utsträckning, är frågan om de inarbetade eller ej inte relevant. För dessa myndigheter är det troligtvis avsaknaden av rutiner som är den främsta anledningen till att rapporteringen av allvarliga IT-incidenter inte sker.

5.2 Bristande interna förutsättningar och förankring?

På vilket sätt och i vilken utsträckning myndigheternas interna förutsättningar och förankring påverkar rapporteringsgraden av allvarliga IT-incidenter till MSB och anmälningar till Polisen, är något som resultatet ger ett tudelat svar på.

Det framgår av resultatet att de interna förutsättningarna har brister gällande informationsdelning till medarbetare och rutiner för överföring av sekretessbelagd information. Det uttalade stödet från ledningsnivå är även det relativt svagt.

Det svaga stödet för informationsspridning till medarbetare kan vara en bidragande orsak till utebliven rapportering, men sannolikt främst i de fall enskilda medarbetare orsakar en IT-incident eller utgör måltavlor för IT-attacker.

Gällande det uttalade stödet från ledningsnivå nyanseras analysen med resultatet för enkätens hypotetiska scenario. Påståendet om att IT-incidentrapportering till MSB skulle kunna utebli på grund av att rapporteringen inte prioriteras på myndigheten, får i enkäten lägst medhåll av samtliga påståenden som presenteras (Figur 11 i avsnitt 4.5). Det resultatet talar för att ett uttalat stöd från ledningsnivå inte har en lika påtaglig negativ inverkan på rapporteringsgraden som resultatet först pekade på.

Figur 11 i avsnitt 4.5 visar dock ett större medhåll för påståendet att *Myndigheten känner sig inte trygg i att sekretessbelagd information lämnar myndighetens kontroll* som en tänkbar orsak till utebliven rapportering. Det svaret kan tolkas utifrån två perspektiv. Det kan antingen betyda att myndigheten inte känner sig trygg med sina egna rutiner för hanteringen av sekretessbelagd information. Eller så är det tänkbart att myndigheten inte känner sig trygg med att den sekretessbelagda informationen hanteras på korrekt sätt hos mottagaren.

Då det inte går att avgöra om myndigheterna syftar på sina egna eller mottagarens rutiner i sina svar, är det svårt säga i vilken utsträckning som stödet för påståendet i det hypotetiska scenariot om hantering av sekretessbelagd information bekräftar slutsatsen att bristande rutiner för överföring av sekretessbelagd information har en negativ inverkan på rapporteringsgraden. Det torde dock vara rimligt att påstå att stödet för påståendet i det hypotetiska scenariot inte talar emot slutsatsen att brister i rutiner för överföring av sekretessbelagd information har en negativ inverkan på rapporteringsgraden.

Slutligen kan det även konstateras att *hög arbetsbelastning på myndigheten vid tillfället för IT-incidenten* är det påstående i det hypotetiska scenariot som näst flest myndigheter uppger som möjlig orsak till utebliven rapportering. Det skulle kunna tolkas som att det vid en IT-incident inte är prioriterat att rapportera till

MSB. Resultatet för påståendet att *rapporteringen inte är en prioriterad uppgift på myndigheten* visar dock att det har, med god marginal, minst antal instämmande myndigheter (Figur 11 i avsnitt 4.5). Det verkar således vara så att det ses som viktigt att rapportera till MSB, men att prioritet nog snarare ligger på att hantera IT-incidenten. Hög arbetsbelastning kan även tänkas påverka rapporteringsgraden indirekt genom att behovet av inarbetade rutiner ökar för att rapporteringen ska klaras av att genomföras under tidspress.

Sammanfattningsvis visar resultatet på att de interna förutsättningar som har en negativ inverkan på rapporteringsgraden av allvarliga IT-incidenter till MSB främst är bristande informationsdelning till medarbetare, bristande rutiner för att hantera överföring av sekretessbelagd information samt hög arbetsbelastning.

5.3 Brister i genomförandet?

Som framgår av resultaten upplever myndigheterna svårigheter i att avgöra vad som utgör en allvarlig IT-incident. Detta gäller framför allt de minsta myndigheterna men även bland de största finns myndigheter som anser att det är svårt. Relaterat till detta visar dessutom enkätresultaten i avsnitt 4.5 att påståendet att *IT-incidenten initialt inte bedömdes vara tillräckligt allvarlig för att behöva rapporteras till MSB* var det som allra flest myndigheter instämde i som en möjlig anledning till att rapportering uteblir.

Det kan finnas flera anledningar till att en incident inte korrekt bedöms som tillräckligt allvarlig. Det kan exempelvis vara svårt att göra en korrekt bedömning om relevant information saknas, eller om man har bristande kunskaper i att avgöra incidenters allvarlighet. De myndigheter som upplever svårigheter i att bedöma IT-incidenters allvarlighet anser dock inte att det tillgängliga stödmaterialet från MSB och CERT-SE på något sätt är mer bristande jämfört med hela svarspopulationen.

Det faktum att myndigheter upplever svårighet kring bedömningen av IT-incidenters allvarlighetsgrad är rimligtvis en bidragande orsak till varför rapportering av inträffade IT-incidenter inte sker. För en myndighet som känner sig osäker på om en inträffad incident ska bedömas som allvarlig eller inte kan det helt enkelt vara en enklare väg att bedöma den som icke allvarlig, speciellt om det samtidigt råder andra omständigheter som försvårar eller inte motiverar rapportering (som hög arbetsbelastning). En ovisshet kring allvarlighetsgraden skulle även i kombination med en eventuell feltolkning av kravet att rapportera IT-incidenter inom 24 timmar kunna leda till att rapportering uteblir. Kanske känner myndigheterna av någon anledning motstånd mot att rapportera en IT-incident vid en tidpunkt som ligger långt senare än tidpunkten då IT-incidenten först upptäcktes. Kravet i föreskrifterna syftar dock på att incidenten ska

rapporteras 24 timmar från det att incidenten bedömdes som *tillräckligt allvarlig*, inte 24 timmar efter att den först *upptäcktes*.

Vad gäller de övriga aspekterna, enkelheten i att avgöra om uppgifter rörande en IT-incident omfattas av sekretess samt enkelheten i att fylla i MSB:s formulär för IT-incidentrapportering, bedöms brister i dessa också som potentiella anledningar till utebliven rapportering, om än i något mindre utsträckning. Överlag anser myndigheterna att det är något enklare att bedöma om incidentuppgifter omfattas av sekretess, än att bedöma om incidenter är allvarliga eller ej. Återigen är det de minsta myndigheterna som upplever de största svårigheterna. Om en myndighet inte känner sig trygg i att avgöra om uppgifter rörande en inträffad IT-incident kan omfattas av sekretess kan det vara en anledning till att rapportering inte sker. Framför allt om myndigheten inte har inarbetade rutiner för att överföra sekretessbelagd information till annan myndighet.

Vad gäller MSB:s formulär för rapportering är det bara 5 procent som *inte alls* eller *i låg grad* instämmer i att det är enkelt att fylla i formuläret. Även för denna aspekt är det de minsta myndigheterna som upplever de största svårigheterna. Relaterat till rapporteringsformuläret visar enkätresultaten också att ett krångligt rapporteringsförfarande var först den sjunde mest angivna möjliga anledningen till att rapportering kan utebli (avsnitt 4.5). Att en upplevd svårighet med att fylla i formuläret skulle utgöra ett *generellt* hinder för att myndigheter rapporterar IT-incidenter verkar därmed mindre troligt.

Sammantaget visar studiens resultat på brister i genomförandet av de bedömningar och arbetsmoment som är nödvändiga för en IT-incidentrapportering. Bristerna i att bedöma allvarlighetsgraden på IT-incidenter bedöms av studieförfattarna vara den starkast bidragande orsaken till att rapportering kan utebli. Svårigheter rörande sekretessbedömning samt att fylla i MSB:s rapporteringsformulär bedöms också som potentiella anledningar, om än något mindre starka i jämförelse.

5.4 Ingen upplevd nytta?

Som framgår av enkätresultaten är det få myndigheter, två procent, som uppger att de inte ser någon nämnvärd nytta med nuvarande IT-incidentrapportering. Det talar emot att en bristfällig motivation skulle vara en starkt bidragande orsak till varför rapportering uteblir. Samtidigt uppger sju procent av myndigheterna att just en upplevd avsaknad av nytta kan vara anledning till utebliven

rapportering.[15] En intressant iakttagelse i sammanhanget är att samtliga av dessa myndigheter, med undantag för en, samtidigt bedömer nyttan med rapporteringen som hög för minst en av de nyttoaspekter som frågas om i enkäten. Det gör resultaten något svårtolkade. Myndigheterna ser nytta med rapporteringen, men bedömer samtidigt att avsaknaden av nytta kan göra att de i samband med en inträffad IT-incident väljer att inte gå vidare med rapportering. För att ytterligare nyansera aspekten om bristfällig motivation är bristande återkoppling från MSB på rapporterade incidenter den fjärde mest angivna anledningen till varför rapportering skulle kunna utebli (se avsnitt 4.5).

Att rapportera allvarliga IT-incidenter är ett obligatorium. Men, om en myndighet inte känner någon större drivkraft till att rapportera, för att den varken upplever några större positiva interna eller externa effekter, är det inte svårt att se att det kan leda till utebliven rapportering. Speciellt som det är upp till myndigheterna själva att avgöra om en incident är så pass allvarlig att den ska rapporteras eller inte.

Den sammantagna bilden är att bristfällig motivation kan vara en förekommande, om än kanske inte den allra största anledningen, till varför rapportering uteblir.

5.5 Andra anledningar?

Det har framkommit anledningar under arbetet med denna studie som inte sorterar under diskussionskapitlets övriga frågeställningar (avsnitt 5.1–5.4), men som likväl kan bidra till att förklara varför rapportering av IT-incidenter inte sker. Att IT-incidentrapporteringen skulle innebära oönskad exponering av myndighetens IT-relaterade problem är en möjlig anledning.[16] Myndigheterna som upplever att oönskad exponering skulle kunna vara en orsak till att inte rapportera är inte många till antalet, men det kan ändå utgöra en viktig faktor för denna grupp.

En annan bidragande anledning till utebliven rapportering är okunskap om rapporteringsskyldigheten. Det är sju myndigheter som svarat *vet ej* på enkätens fråga huruvida myndigheten är rapporteringsskyldig. Det är möjligt att de svarande varit osäkra på huruvida myndighetens interna IT-drift är utkontrakterad och myndigheten därmed under dessa premisser är undantagen

[15] Ingen upplevd nytta var den sjätte mest angivna möjliga anledningen till varför rapportering skulle kunna utebli (se Figur 11 i avsnitt 4.5).

[16] Att rapportering medför oönskad exponering av myndighetens IT-relaterade problem är den tionde mes angivna möjliga anledningen till varför rapportering skulle kunna utebli (se Figur 11 i avsnitt 4.5).

rapporteringsskyldighet.[17] Det kan även bero på bristande kännedom om MSB:s föreskrifter, vilket kan påverka dessa sju myndigheters rapportering av IT-incidenter till MSB.

En tredje anledning som kan bidra till att förklara den rådande rapporteringsfrekvensen är upplevda oklarheter gällande värdmyndigheters roll och ansvar gentemot MSB och den myndighet som denne agerar värd åt. Som framkommit upplevs det finnas oklarheter angående rapporteringen av allvarliga IT-incidenter till MSB – gällande både förväntningar på värdmyndigheten och ansvar gentemot MSB.

Flera myndigheter som kontaktade studieförfattarna i och med utskicket av enkäten hade en förväntan att rapportering av eventuella allvarliga IT-incidenter till MSB sköts av deras värdmyndighet då det är denne som har kontroll över IT-miljön och även är den som hanterar en eventuell incident. Det upplevdes även vara oklart huruvida rapportering enbart ska göras för värdmyndigheten eller även för de myndigheterna vars IT-miljöer hanteras om en IT-incident inträffar i värdmyndighetens IT-miljö.

Ett ytterligare fall som noterats i och med enkätutskicket är då en myndighet har en värdmyndighet som är undantagen från den obligatoriska IT-incidentrapportering, exempelvis Regeringskansliet. De myndigheter, vars värdmyndighet inte ska rapportera IT-incidenter, hamnar mellan stolarna. Enligt MSB:s statistik räknas dessa som rapporteringsskyldiga, men i praktiken är de inte det. Här uppstår således en situation där dessa myndigheter har räknats med i statistiken över rapporteringsskyldiga, men det kan alltså vara något som ger en missvisande bild.

5.6 Varför uteblir polisanmälan?

För att en myndighet ska ha nödvändiga förutsättningar för att kunna polisanmäla en allvarlig IT-incident så krävs motsvarande förutsättningar som för rapporteringen av IT-incidenter till MSB. Det krävs exempelvis att myndigheten har rutiner för att kunna identifiera, bedöma, hantera och dokumentera IT-incidenter. Först när rutiner för dessa första fyra steg finns på plats blir det aktuellt med rutiner för att genomföra själva polisanmälan. Resonemanget i 5.1 kring bristande rutiner är således även relevant när det gäller polisanmälan av IT-incidenter.

[17] Undantag gäller för myndigheter som har delar av sin IT-drift utkontrakterad till en ickestatlig aktör och avtalet för detta omförhandlades innan april 2016 då MSB:s föreskrifter om incidentrapportering (9§ MSBFS 2016:2) trädde i kraft.

På samma sätt som för rapportering till MSB så är för polisanmälan *ej inarbetade rutiner* en av de mest uttalade anledningarna till att polisanmälan kan utebli. Det blir således även tydligt i detta sammanhang att det inte bara krävs att rutiner finns, utan de behöver även vara inarbetade för att de ska ge ett stöd i ett skarpt läge. För myndigheter som har varit förskonade från IT-incidenter med ursprung i brottsliga gärningar, och därmed inte har behövt använda rutinerna, kan det vara relevant att öva på att använda rutinerna.

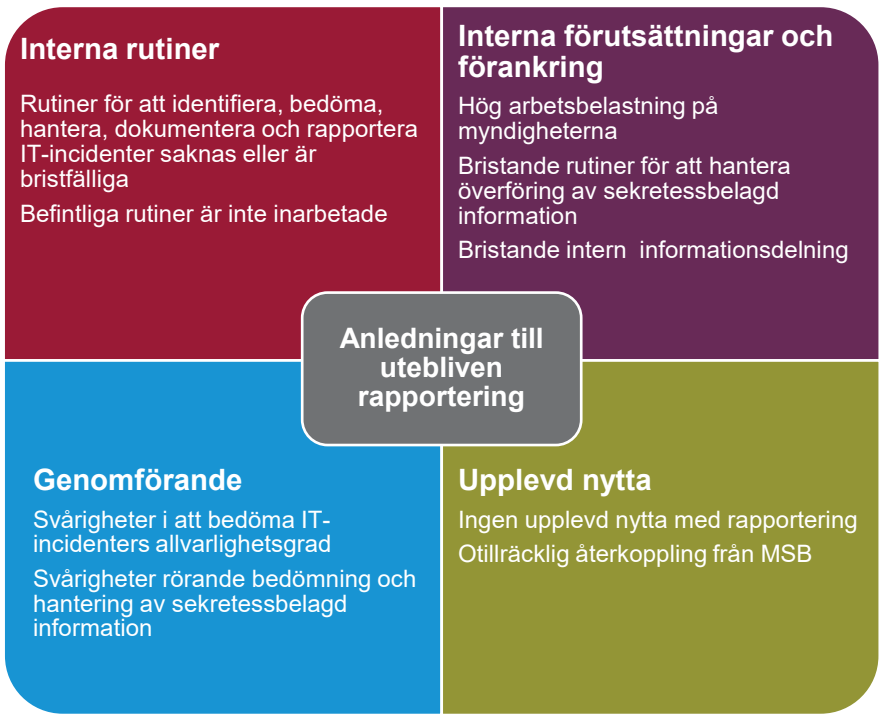
En ytterligare nödvändig förutsättning är att kunna bedöma om en inträffad IT-incident är allvarlig. När det gäller polisanmälan spelar troligtvis själva bedömningen av huruvida IT-incidenten har sitt ursprung i en brottslig gärning en viktigare roll, men incidentens allvarlighet bör även kunna påverka viljan att polisanmäla. Resultaten som framkom i avsnitt 4.3 tyder på att majoriteten av myndigheterna inte upplever det som svårt att avgöra om en IT-incident ska polisanmälas. Samtidigt visar det hypotetiska scenariot om polisanmälan (avsnitt 4.6) på att den mest uttryckta anledningen till att polisanmälan kan utebli är att *IT-incidenten initialt inte bedömdes vara tillräckligt allvarlig för att behöva polisanmälas*.

Något som dock skiljer polisanmälan från rapporteringen till MSB är att nyttan med att polisanmäla upplevs vara lägre. Just att det inte upplevs vara någon nytta med att polisanmäla en inträffad IT-incident som har sitt ursprung i en brottslig gärning är den tredje mest uttryckta anledningen till att polisanmälan kan utebli.

Den sammantagna bilden av varför myndigheter inte polisanmäler IT-incidenter som har sitt ursprung i en brottslig gärning är att IT-incidenter initialt kanske inte bedöms vara tillräckligt allvarliga, att rutiner för att polisanmäla dem inte är inarbetade samt att inte upplevs finnas någon nytta med att göra en polisanmälan.

6 Slutsatser

Studiens resultat visar att det inte finnas någon anledning som ensamt förklarar den bedömt låga rapporteringsgraden av allvarliga IT-incidenter till MSB. Istället visar studien att det finns flera olika anledningar som enskilt och i samspel med varandra bidrar till att myndigheters rapportering av allvarliga IT-incidenter kan utebli. För att återkoppla till studiens analysramverk presenteras i Figur 15 de anledningar som tydligast framträtt.



Figur 15: Övergripande bild av identifierade anledningar till varför rapportering av IT-incidenter till MSB kan utebli.

Utöver slutsatserna som framkommer i Figur 15 har även oklarheter kring rapporteringsskyldighet och otydligheter gällande ansvarsfördelning i relationen mellan små myndigheter och deras värdmyndigheter, visat sig vara anledningar som kan påverka rapporteringsgraden.

Det är viktigt att ha i åtanke att de rapporteringsskyldiga myndigheterna inte är en homogen grupp. Myndigheterna skiljer sig åt i många avseenden. Därför är inte alla anledningar till utebliven rapportering relevanta i samma utsträckning

för alla myndigheter. Som resultaten och diskussionen visar är en del anledningar mer framträdande bland mindre myndigheter, exempelvis bristen på interna rutiner och svårigheten att bedöma IT-incidentens allvarlighetsgrad, medan det i andra fall inte finns någon koppling till myndighetens storlek. Resultaten tyder dock på att det är lika stor andel bland små myndigheter som bland stora myndigheter (ungefär hälften) som uppger att det finns potentiella anledningar till att rapportering av allvarliga IT-incidenter till MSB kan utebli.

På motsvarande sätt som för utebliven rapportering är slutsatsen för utebliven polisanmälan av IT-incidenter med ursprung i brottslig gärning att det inte finns ett enskilt svar. Även för denna fråga visar studien på att det är flertalet anledningar som enskilt och tillsammans bidrar till att förklara den rådande anmälningsfrekvensen. Följande tre anledningar betonades starkare än andra: att en IT-incident initialt inte bedöms vara tillräckligt allvarlig för att polisanmälas, att rutiner för att polisanmäla IT-incidenter inte är inarbetade, samt att det inte upplevs finnas någon nytta med att göra en polisanmälan.

6.1 Förslag på fortsatta studier

Den här studien har haft ett brett angreppssätt med ambition att nå samtliga rapporteringsskyldiga myndigheter genom en allomfattande enkätundersökning. Det dataunderlag som samlats in har möjliggjort för att dra slutsatser utifrån ett mer övergripande perspektiv. För den fortsatta kunskapsuppbyggnaden gällande myndigheters rapportering och polisanmälan av allvarliga IT-incidenter bör studien kompletteras med en kvalitativ ansats. Mer djuplodade intervjuer skulle exempelvis kunna nyansera och konkretisera slutsatserna som dras i denna studie.

Ett intressant spår att följa som framkommit av denna studie är skillnaderna i förutsättningar mellan olika kategorier (storleksmässigt) av myndigheter att uppfylla den obligatoriska IT-incidentrapporteringen. Det är en studie som skulle kunna bidra till att utforma åtgärder för att öka rapporteringsgraden.

Slutligen har även myndigheterna bidragit med förbättringsförslag genom fritextsvar i enkätundersökningen (se Bilaga C). Dessa kan ge värdefulla uppslag på handlingsvägar framåt för en förbättrad rapporteringsgrad.

Referenser

CERT-SE (u.å.). https://www.cert.se/it-incidentrapportering/om-it-incidentrapportering/. Hämtad 2019-11-11.

Finansdepartementet (2007). *Myndighetsförordning (2007:515)*

Justitiedepartementet (2009). *Offentlighets- och sekretesslag (2009:400)*.

Justitiedepartementet (2015a). *Regeringen inför krav på IT-incidentrapportering för statliga myndigheter*. Pressmeddelande 2015-12-17. https://www.regeringen.se/pressmeddelanden/2015/12/regeringen-infor-krav-pa-it-incidentrapportering-for-statliga-myndigheter/. Hämtad 2019-11-11

Justitiedepartementet (2015b). *Förordning (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap*.

Myndigheten för samhällsskydd och beredskap (2019). *Årsrapport It-incidentrapportering 2018*, Publ.nr. MSB1334 – April 2019

Myndigheten för samhällsskydd och beredskap (2018). *Årsrapport It-incidentrapportering 2017*, Publ.nr. MSB1198 – April 2018

Myndigheten för samhällsskydd och beredskap (2017). *Årsrapport It-incidentrapportering 2016*, Diarienr. 2016-6304-7, Mars 2017

Myndigheten för samhällsskydd och beredskap (2016a). *Exempel på it-incidenter – Typexempel inklusive bedömning*. https://www.cert.se/it-incidentrapportering/Exempel%20p%C3%A5%20it-incidenter%20april%202016.pdf. Hämtad 2019-05-20.

Myndigheten för samhällsskydd och beredskap (2016b). *Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet.* MSBFS 2016:1.

Myndigheten för samhällsskydd och beredskap (2016c). *Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters rapportering av it-incidenter.* MSBFS 2016:2.

Statistiska centralbyrån (u.å.). http://www.myndighetsregistret.scb.se/. Hämtad 2019-04-01.

Bilaga A. Följebrev och enkät

I avsnitten som följer återges det följebrev och den enkät som skickades ut till de rapporteringsskyldiga myndigheterna.

A.1 Följebrev

Hej,

Den bifogade enkäten är avsedd för den person på myndigheten som ansvarar för, eller är insatt i, rapporteringen av inträffade IT-incidenter till MSB i enlighet med 20 § i *Förordningen (2015:1052) om krisberedskap och bevakningsansvariga myndigheters åtgärder vid höjd beredskap*. Besvarad enkät önskas i retur senast 2019-06-20.

Vänliga hälsningar,

Ann-Sofie Stenérus Dover

Totalförsvarets forskningsinstitut

A.2 Enkät

Undersökning om myndigheters rapportering av IT-incidenter

Totalförsvarets forskningsinstitut (FOI) genomför på uppdrag av Justitiedepartementet en studie kring myndigheters rapportering av IT-incidenter till MSB. För att få en förståelse för rapporteringsskyldiga myndigheters syn på rapporteringen av IT-incidenter genomförs en enkätundersökning. Denna enkätundersökning skickas till samtliga myndigheter som är skyldiga att skyndsamt rapportera IT-incidenter till MSB enligt 20 § i förordning 2015:1052 och riktar sig till den person vid myndigheten som ansvarar för, eller är insatt i, denna rapportering.

Myndigheternas rapporteringsskyldighet omfattar IT-incidenter som inträffar i deras informationssystem och som allvarligt kan påverka säkerheten i den informationshantering som myndigheten ansvarar för, eller som inträffar i tjänster som myndigheten tillhandahåller åt en annan organisation.

Dina svar är viktiga

Vi uppskattar om du tar dig tid att besvara enkäten så snart som möjligt. Dina svar är betydelsefulla och bidrar till att resultaten blir mer tillförlitliga. Svar från såväl stora som små myndigheter är viktigt för att få en rättvisande bild. Detta gäller även de myndigheter vars IT-drift är utkontrakterad till antingen privat aktör eller annan statlig myndighet.[18] Med din medverkan bidrar du till kunskap om hur rapporteringen av IT-incidenter fungerar idag och hur den i förlängningen kan förbättras för att fungera ännu bättre.

Resultaten från enkätundersökningen kommer att rapporteras till Justitiedepartementet i slutet av 2019. Även MSB kommer att få ta del av resultaten.

Så här gör du

Besvara pappersenkäten och skicka in den i det portofria svarskuvertet. Vi ber dig besvara frågorna så snart som möjligt. **Sista svarsdatum är 2019-06-20**. När det i enkäten refereras till hur myndigheten ser på något avses den myndighet du representerar och hur du upplever att man på myndigheten ser på aktuell fråga.

Skydd av lämnade uppgifter

För att du som respondent ska känna dig helt trygg i besvarandet av enkätfrågorna genomförs undersökningen med hjälp av anonyma enkäter. Enkäten har ingen märkning som identifierar dig som respondent. Inga personuppgifter kommer att behandlas.

Var noga med att du i enkätens fritextfrågor inte anger information som omfattas av sekretess eller kan användas för att identifiera den myndighet du representerar. Har du frågor om enkäten är du välkommen att kontakta Ann-Sofie Stenérus Dover (ann-sofie.stenerus.dover@foi.se alternativt via FOI:s växel 08-55 50 30 00).

Stort tack för din medverkan!

Med vänlig hälsning

Ann-Sofie Stenérus Dover

Projektledare
FOI

[18] Myndigheter är undantagna rapporteringsskyldigheten i de fall en myndighet har delar av sin IT-drift utkontrakterad till en ickestatlig aktör och avtalet för detta omförhandlades innan april 2016 då MSB:s föreskrifter om incidentrapportering (9§ MSBFS 2016:2) trädde i kraft.

Bakgrund

1. **Är myndigheten en bevakningsansvarig myndighet?**
   - ☐ **Ja**
   - ☐ **Nej**
   - ☐ **Vet ej**

Om du har svarat Ja på fråga 1 vänligen gå vidare till fråga 3.

2. **Hur stor är myndigheten?**
   Besvara enbart frågan om myndigheten inte är bevakningsansvarig.
   - ☐ **Fler än 1000 anställda**
   - ☐ **301–1000 anställda**
   - ☐ **101–300 anställda**
   - ☐ **26–100 anställda**
   - ☐ **0–25 anställda**

3. **Är myndigheten skyldig att rapportera IT-incidenter enligt 20 § i förordning 2015:1052? Myndigheter kan i nuläget vara undantagna rapporteringsskyldigheten i de fall delar av IT-driften är utkontrakterad och avtalet för detta omförhandlades innan april 2016 då MSB:s föreskrifter om incidentrapportering (MSBFS 2016:2) trädde i kraft.**
   - ☐ **Ja**
   - ☐ **Nej**
   - ☐ **Vet ej**

Om du har svarat Nej på fråga 3 och myndigheten inte frivilligt rapporterar IT-incidenter till MSB, vänligen gå vidare till fråga 11.

Myndighetens rapportering av IT-incidenter

4. **Hur väl stämmer nedanstående påståenden in på myndigheten? Myndigheten har interna rutiner för hur IT-incidenter ska…**

		Instämmer inte alls	Instäm-mer i låg grad	Instäm-mer delvis	Instämmer i hög grad	Instäm-mer helt	Vet ej
a)	identifieras	☐	☐	☐	☐	☐	☐
b)	bedömas	☐	☐	☐	☐	☐	☐
c)	hanteras	☐	☐	☐	☐	☐	☐
d)	dokumenteras	☐	☐	☐	☐	☐	☐
e)	rapporteras	☐	☐	☐	☐	☐	☐

5. **Hur väl stämmer nedanstående påståenden in på myndigheten? På myndigheten…**

		Instämmer inte alls	Instämmer i låg grad	Instämmer delvis	Instämmer i hög grad	Instämmer helt	Vet ej
a)	… har det tillhandahållits information till myndighetens medarbetare om krav på myndigheten att rapportera IT-incidenter till MSB.	☐	☐	☐	☐	☐	☐
b)	… finns det en utpekad ansvarig för hanteringen av IT-incidentrapporteringen till MSB.	☐	☐	☐	☐	☐	☐
c)	… finns det resurser för att hantera rapporteringen av IT-incidenter till MSB.	☐	☐	☐	☐	☐	☐
d)	… är det uttalat från ledningsnivå att det är viktigt att IT-incidenter rapporteras till MSB.	☐	☐	☐	☐	☐	☐

6. **Hur väl stämmer nedanstående påståenden in på myndigheten? På myndigheten anses att…**

		Instämmer inte alls	Instämmer i låg grad	Instämmer delvis	Instämmer i hög grad	Instämmer helt	Vet ej
a)	… det är enkelt att avgöra vad som utgör en allvarlig IT-incident som ska rapporteras till MSB.	☐	☐	☐	☐	☐	☐
b)	… det är enkelt att avgöra när en IT-incident ska polisanmälas.	☐	☐	☐	☐	☐	☐
c)	… det är enkelt att avgöra om uppgifter rörande en IT-incident omfattas av sekretess.	☐	☐	☐	☐	☐	☐
d)	… det finns inarbetade rutiner för överföring av sekretessbelagd information mellan myndigheter.	☐	☐	☐	☐	☐	☐
e)	… det finns tillräckligt med stödmaterial från MSB och CERT-SE för att myndigheten ska kunna uppfylla kravet på rapportering av IT-incidenter[19].	☐	☐	☐	☐	☐	☐
f)	… det är enkelt att fylla i MSB:s formulär för IT-incidentrapportering.	☐	☐	☐	☐	☐	☐

[19] Såsom exempelvis MSB:s föreskrift MSBFS 2016:2 om statliga myndigheters rapportering av IT-incidenter, skriften ”Exempel på IT-incidenter – Typexempel inklusive bedömning” utgiven av MSB, samt information och FAQ om IT-incidentrapporteringen på www.cert.se.

7. **Hur väl stämmer nedanstående påståenden in på myndigheten? På myndigheten upplevs nyttan med myndigheternas rapportering av IT-incidenter till MSB vara att…**

		Instämmer inte alls	Instämmer i låg grad	Instämmer delvis	Instämmer i hög grad	Instämmer helt	Vet ej
a)	… andra myndigheter som riskerar att drabbas av motsvarande IT-incident kan varnas.	☐	☐	☐	☐	☐	☐
b)	… bli förvarnad om inträffade IT-incidenter hos andra myndigheter.	☐	☐	☐	☐	☐	☐
c)	… ge underlag till MSB:s lägesbild.	☐	☐	☐	☐	☐	☐
d)	… handla i enlighet med myndighetens rapporterings-skyldighet.	☐	☐	☐	☐	☐	☐
e)	… bidra till att öka svenska myndigheters IT-säkerhetsnivå.	☐	☐	☐	☐	☐	☐
f)	… det ökar medvetenheten internt inom myndigheten om IT-incidenter.	☐	☐	☐	☐	☐	☐

Nyttan med rapportering av IT-incidenter

8. **Ser du annan nytta för myndigheten med rapporteringen av IT-incidenter än förslagen i fråga 7?**

Hypotetiska scenarier

9. **Om det vid myndigheten skulle inträffa en <u>allvarlig IT-incident</u>, i vilken utsträckning skulle något eller några av följande påståenden kunna vara anledningar till att <u>rapportering till MSB inte sker</u>?**

		Instämmer inte alls	Instämmer i låg grad	Instämmer delvis	Instämmer i hög grad	Instämmer helt	Vet ej
a)	Själva rapporteringsförfarandet att fylla i och mejla incident-rapportmallen till CERT-SE är krångligt.	☐	☐	☐	☐	☐	☐

9. **Om det vid myndigheten skulle inträffa en <u>allvarlig IT-incident</u>, i vilken utsträckning skulle något eller några av följande påståenden kunna vara anledningar till att <u>rapportering till MSB inte sker</u>?**

		Instämmer inte alls	Instämmer i låg grad	Instämmer delvis	Instämmer i hög grad	Instämmer helt	Vet ej
b)	Att rapportera IT-incidenter till MSB medför merarbete för myndigheten.	☐	☐	☐	☐	☐	☐
c)	Hög arbetsbelastning på myndigheten vid tillfället för IT-incidenten.	☐	☐	☐	☐	☐	☐
d)	Myndigheten får inte tillräcklig återkoppling på IT-incidenter som rapporteras till MSB.	☐	☐	☐	☐	☐	☐
e)	Att rapportera IT-incidenter till MSB är inte en prioriterad uppgift på myndigheten.	☐	☐	☐	☐	☐	☐
f)	Myndigheten upplever inte någon nytta med att rapportera IT-incidenten till MSB.	☐	☐	☐	☐	☐	☐
g)	Myndigheten känner sig inte trygg i att sekretessbelagd information lämnar myndighetens kontroll.	☐	☐	☐	☐	☐	☐
h)	Att rapportera IT-incidenter till MSB kan medföra oönskad exponering av myndighetens IT-relaterade problem.	☐	☐	☐	☐	☐	☐
i)	Myndigheten saknar rutiner för att rapportera IT-incidenter.	☐	☐	☐	☐	☐	☐
j)	Myndighetens rutiner för att rapportera IT-incidenter är inte inarbetade.	☐	☐	☐	☐	☐	☐

9. **Om det vid myndigheten skulle inträffa en allvarlig IT-incident, i vilken utsträckning skulle något eller några av följande påståenden kunna vara anledningar till att rapportering till MSB inte sker?**

		Instämmer inte alls	Instämmer i låg grad	Instämmer delvis	Instämmer i hög grad	Instämmer helt	Vet ej
k)	IT-incidenten bedöms initialt inte vara tillräckligt allvarlig för att behöva rapporteras till MSB.	☐	☐	☐	☐	☐	☐
l)	Nödvändig kompetens för att rapportera IT-incidenter saknas på grund av omsättning av nyckelpersoner.	☐	☐	☐	☐	☐	☐

10. **Om det vid myndigheten skulle inträffa en allvarlig IT-incident som har sitt ursprung i en brottslig gärning, i vilken utsträckning skulle något eller några av följande påståenden kunna vara anledningar till att IT-incidenten inte polisanmäls?**

		Instämmer inte alls	Instämmer i låg grad	Instämmer delvis	Instämmer i hög grad	Instämmer helt	Vet ej
a)	Att polisanmäla IT-incidenter medför merarbete för myndigheten.	☐	☐	☐	☐	☐	☐
b)	Att polisanmäla IT-incidenter är inte en prioriterad uppgift på myndigheten.	☐	☐	☐	☐	☐	☐
c)	IT-incidenten bedöms initialt inte vara tillräckligt allvarlig för att behöva polisanmälas.	☐	☐	☐	☐	☐	☐
d)	Myndigheten upplever ingen nytta med att polisanmäla IT-incidenten.	☐	☐	☐	☐	☐	☐

10. **Om det vid myndigheten skulle inträffa en allvarlig IT-incident som har sitt ursprung i en brottslig gärning, i vilken utsträckning skulle något eller några av följande påståenden kunna vara anledningar till att IT-incidenten inte polisanmäls?**

		Instämmer inte alls	Instämmer i låg grad	Instämmer delvis	Instämmer i hög grad	Instämmer helt	Vet ej
e)	Hög arbetsbelastning på myndigheten vid tillfället för IT-incidenten.	☐	☐	☐	☐	☐	☐
f)	Myndigheten saknar rutiner för att polisanmäla IT-incidenter.	☐	☐	☐	☐	☐	☐
g)	Myndighetens rutiner för att polisanmäla IT-incidenter är inte inarbetade.	☐	☐	☐	☐	☐	☐
h)	Att polisanmäla IT-incidenter kan medföra oönskad exponering av myndighetens IT-relaterade problem.	☐	☐	☐	☐	☐	☐
i)	Nödvändig kompetens för att polisanmäla IT-incidenter saknas på grund av omsättning av nyckelpersoner.	☐	☐	☐	☐	☐	☐

Övriga kommentarer

11. **Anser du att MSB bör förändra något avseende IT-incidentrapporteringen för att myndigheten ska börja rapportera eller öka rapporteringen av IT-incidenter?**
Förändringsförslag kan exempelvis avse nuvarande stödmaterial eller rapporteringsförfarande.

12. **Har du några ytterligare synpunkter eller kommentarer som inte fångas upp av enkäten?**

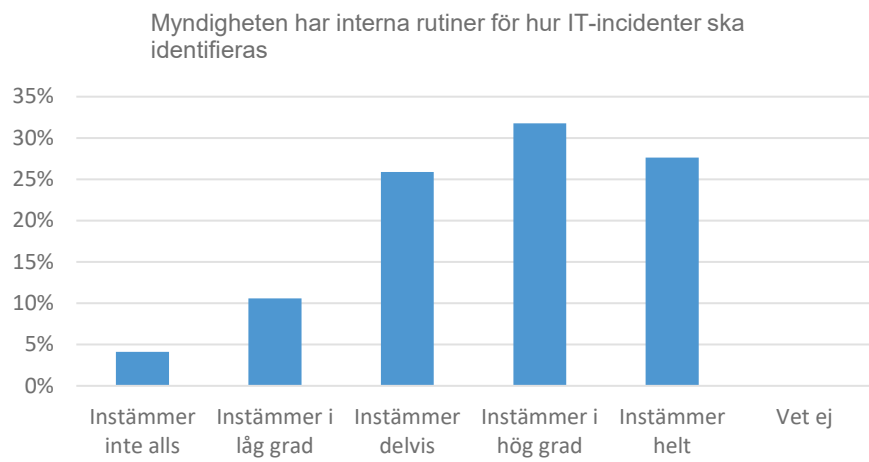
Bilaga B. Enkätresultat

I denna bilaga redovisas resultaten för enkätens frågor 4–7 samt 9–10. Övriga enkätsvar redovisas enligt följande: resultaten för fråga 1–3 redovisas i inledningen av kapitel 4, en sammanställning av fritextsvaren till fråga 8 redovisas i avsnitt 4.4, och en sammanställning av fritextsvaren till fråga 11 och 12 i Bilaga C.

B.1 Interna rutiner

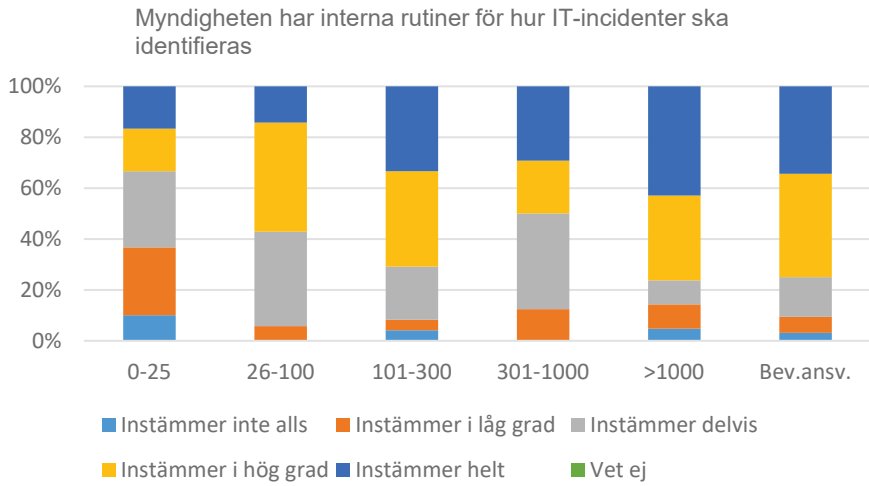
B.1.1 Interna rutiner för att identifiera IT-incidenter

Enkätresultaten visar att 60 procent av myndigheterna instämmer *i hög grad* eller *helt* i påståendet om att myndigheten har rutiner för att identifiera IT-incidenter. Motsvarande procentsats för de som uppger att de *inte alls* eller *i låg grad* instämmer är 15 procent.



Figur 1: Fördelning av hur väl myndigheterna instämmer med att de har en rutin för att *identifiera* IT-incidenter.

Den största andelen myndigheter som angett att de *i hög grad* eller *helt* instämmer återfinns bland myndigheter med fler än 1000 anställda samt bevakningsansvariga myndigheter. Bland dessa uppger 76 respektive 75 procent att de instämmer *i hög grad* eller *helt* i påstående att de har interna rutiner för hur IT-incidenter ska identifieras. Tätt följt är myndigheter med 101-300 anställda där andelen uppgår till 71 procent.



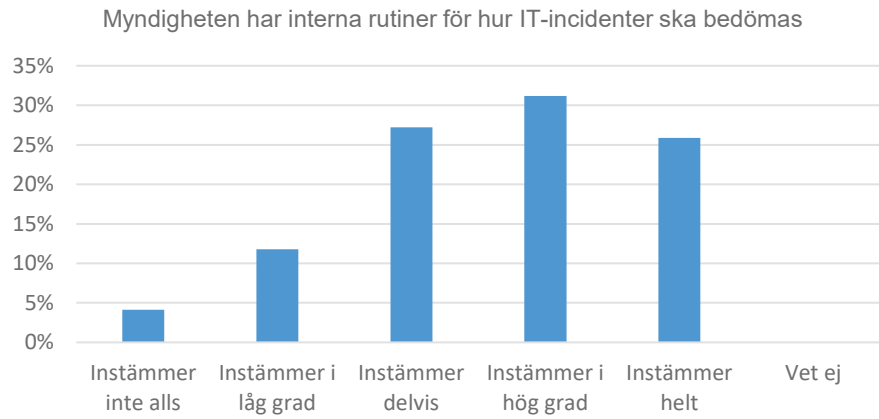
Figur 2: Fördelning av hur väl myndigheterna instämmer med att de har en rutin för att *identifiera* IT-incidenter grupperat efter myndighetskategorier.

Myndighetsgruppen med lägst andel som instämmer *i hög grad* eller *helt* är den med 0-25 anställda där andelen är 34 procent. Näst lägst andel återfinns hos myndigheter med 301-1000 anställda med 50 procent.

Andelen myndigheter som uppger att de *inte alls* eller *i låg grad* instämmer är störst i kategorin med 0-25 anställda. I denna uppgår andelen till 37 procent. Hos bevakningsansvariga myndigheter är motsvarande andel 14 procent, och för 301-1000 anställda uppnår densamma till 13 procent. Hos övriga ligger andelen på mellan 6 och 9 procent.

B.1.2 Interna rutiner för att bedöma IT-incidenter

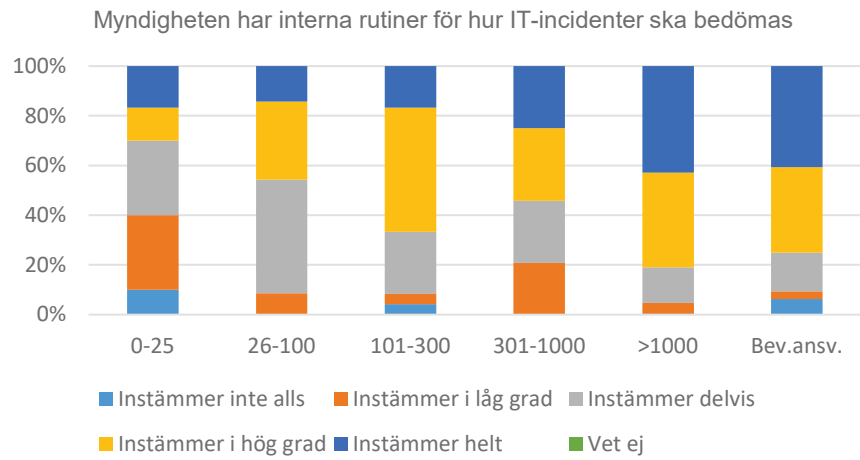
I resultatet för samtliga myndigheter uppger 57 procent att de instämmer *i hög grad* eller *helt* i påståendet att myndigheten har interna rutiner för hur IT-incidenter ska bedömas. Motsvarande siffra för svarsalternativen instämmer *inte alls* eller instämmer *i låg grad* är 16 procent.



Figur 3: Fördelning av hur väl myndigheterna instämmer med att de har en rutin för att *bedöma* IT-incidenter.

Störst andel myndigheter som instämmer *i hög grad* eller *helt* i påståendet att myndigheten har interna rutiner för hur IT-incidenter ska bedömas finns hos myndigheter med fler än 1000 anställda samt bevakningsansvariga myndigheter. Andelen uppgår till 81 respektive 75 procent.

Myndigheter med 0-25 anställda är den myndighetskategori med lägst andel som instämmer *i hög grad* eller *helt*, med en andel om 30 procent.

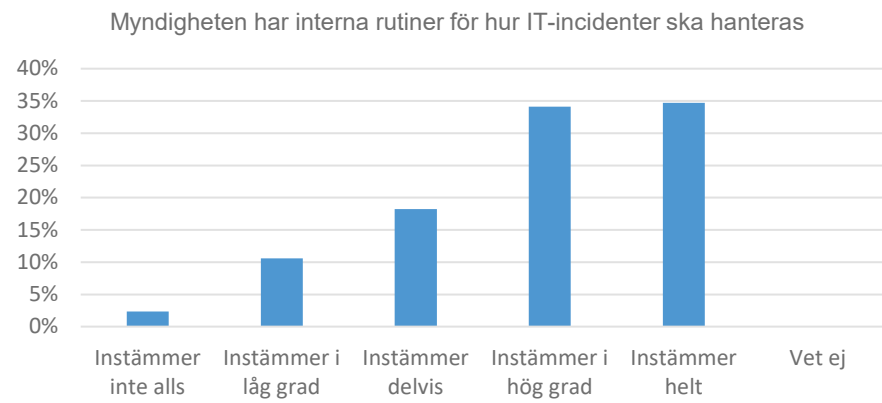


Figur 4: Fördelning av hur väl myndigheterna instämmer med att de har en rutin för att *bedöma* IT-incidenter grupperat efter myndighetskategorier.

Störst andel myndigheter som anger *instämmer inte alls* eller *i låg grad* i påståendet om rutiner för att bedöma IT-incidenter återfinns hos de minsta myndigheterna (0-25 anställda) med en andel om 40 procent. Hos myndigheter med 301-1000 anställda uppges 21 procent instämma *i låg grad* eller *inte alls*. Hos övriga kategorier är motsvarande siffra mellan 6 och 9 procent.

B.1.3 Interna rutiner för att hantera IT-incidenter

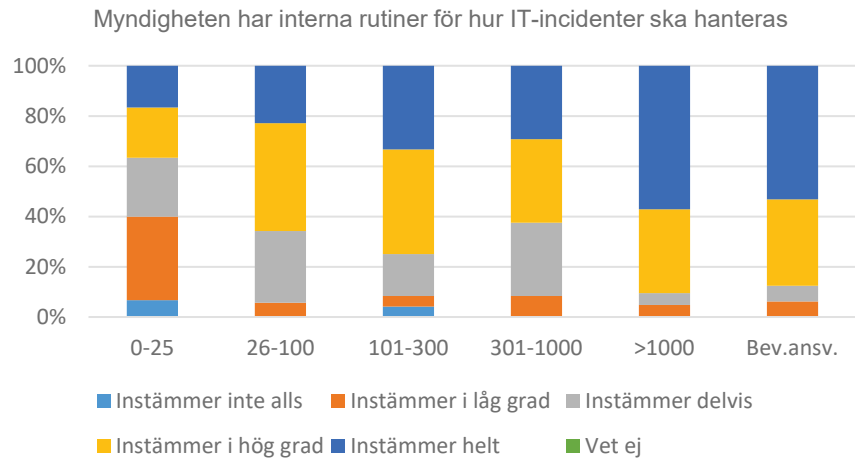
För samtliga myndigheter uppger 69 procent att de instämmer *i hög grad* eller *helt* i påståendet att myndigheten har interna rutiner för att hantera IT-incidenter. Motsvarande siffra för svarsalternativen *instämmer inte alls* och *instämmer i låg grad* är 13 procent.



Figur 5: Fördelning av hur väl myndigheterna instämmer med att de har en rutin för att *hantera* IT-incidenter.

De myndigheter där störst andel har angett att de instämmer *i hög grad* eller *helt* i påståendet att de har interna rutiner för att hantera IT-incidenter tillhör kategorierna myndigheter med fler än 1000 anställda samt bevakningsansvariga myndigheter. Hos dessa grupper svarar 90 respektive 87 procent att de instämmer *i hög grad* eller *helt*. Lägst andel återfinns hos de minsta myndigheterna (0-25 anställda) med 37 procent.

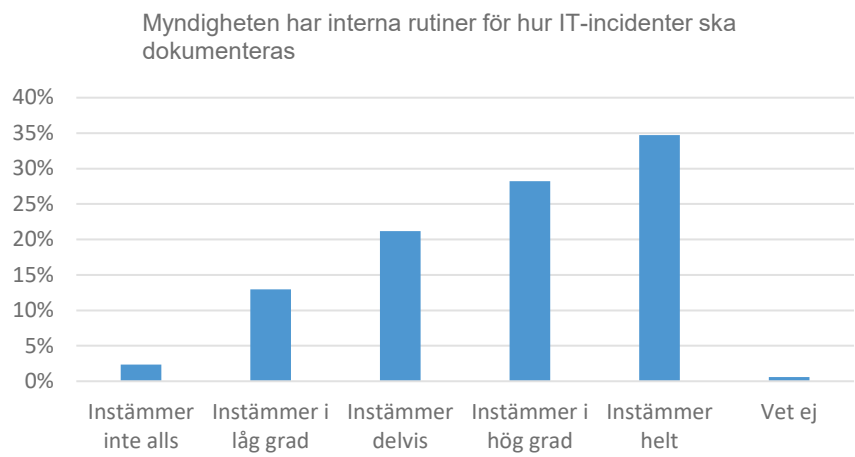
Störst andel som *inte alls* eller *i låg grad* instämmer återfinns hos de minsta myndigheterna (0-25 anställda), där 40 procent har valt dessa alternativ. Hos övriga myndighetskategorier uppger 5-8 procent att de *inte instämmer alls* eller *i låg grad*.



Figur 6: Fördelning av hur väl myndigheterna instämmer med att de har en rutin för att *hantera* IT-incidenter grupperat efter myndighetskategorier.

B.1.4 Interna rutiner för att dokumentera IT-incidenter

För samtliga myndigheter uppger 63 procent att de instämmer *i hög grad* eller *helt* i påståendet att myndigheten har interna rutiner för att dokumentera IT-incidenter. Motsvarande siffra för de som *inte instämmer alls* eller *i låg grad* är 15 procent.

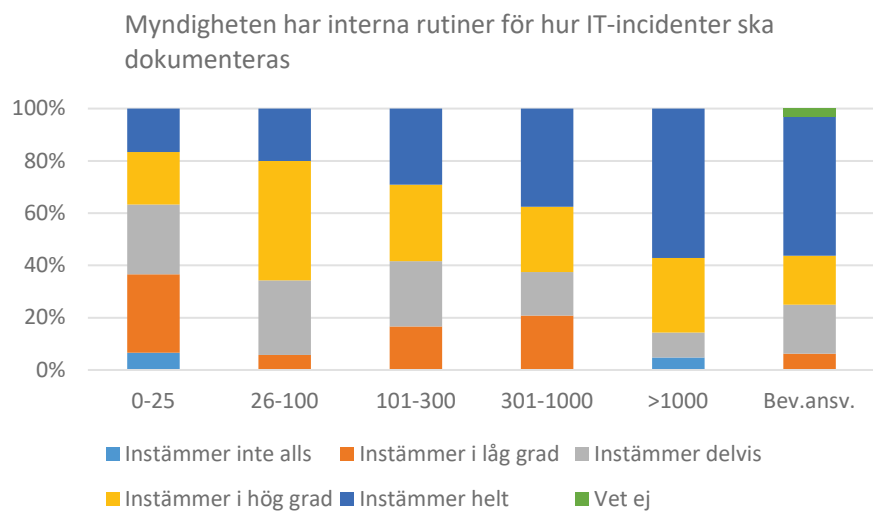


Figur 7: Fördelning av hur väl myndigheterna instämmer med att de har en rutin för att *dokumentera* IT-incidenter.

Den myndighetskategori där störst andel anser sig ha interna rutiner för hur IT-incidenter ska dokumenteras är myndigheter med fler än 1000 anställda. Bland dessa instämmer 86 procent *i hög grad* eller *helt*.

Den myndighetskategori där lägst andel myndigheter har angett att de instämmer *i hög grad* eller *helt* är den med 0-25 anställda. I denna grupp är det 37 procent som instämmer *i hög grad* eller *helt*.

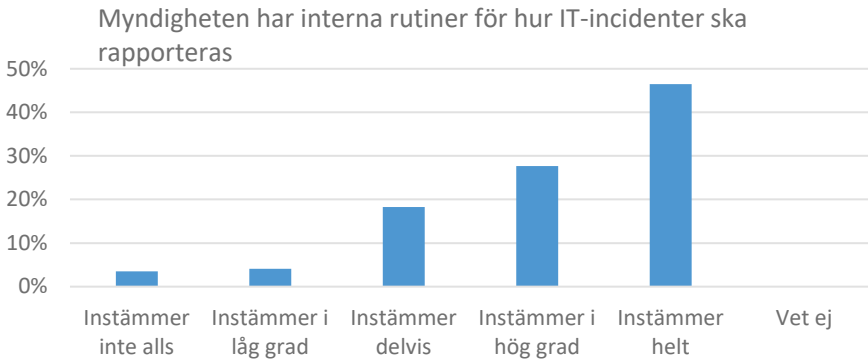
Det är även bland de minsta myndigheterna som störst andel har valt svarsalternativen *instämmer inte alls* eller *i låg grad* med 37 procent. Därefter följer myndigheter med 301-1000 anställda med 21 procent, samt myndigheter med 101-300 anställda med 17 procent.



Figur 8: Fördelning av hur väl myndigheterna instämmer med att de har en rutin för att *dokumentera* IT-incidenter grupperat efter myndighetskategorier.

B.1.5 Interna rutiner för att rapportera IT-incidenter

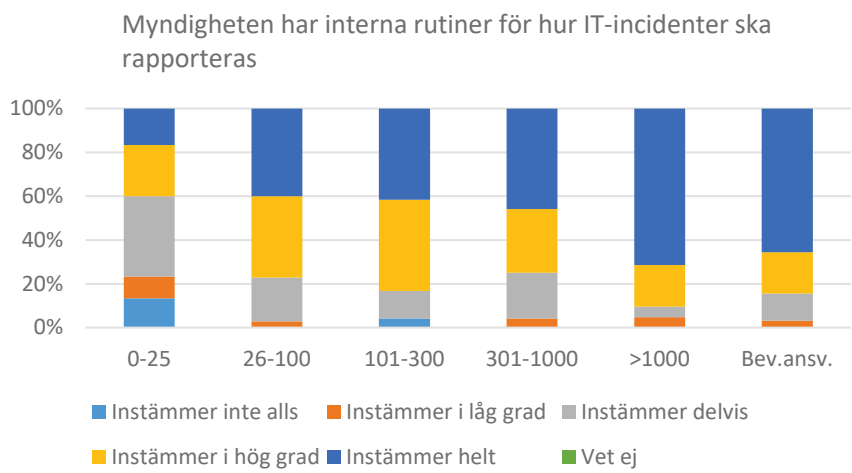
För samtliga myndigheter uppger 74 procent att de instämmer *i hög grad* eller *helt* i påståendet att myndigheten har interna rutiner för att rapportera IT-incidenter. Motsvarande siffra för de som *inte instämmer alls* eller *i låg grad* är 8 procent.



Figur 9: Fördelning av hur väl myndigheterna instämmer med att de har en rutin för att *rapportera* IT-incidenter.

De myndigheter där störst andel instämmer *i hög grad* eller *helt* är de med fler än 1000 anställda, med en andel om 90 procent. Bevakningsansvariga myndigheter samt myndigheter med 101-300 anställda ligger i närheten med 85 respektive 84 procent. Myndighetskategorin där lägst andel myndigheter instämmer *i hög grad* eller *helt* är de med 0-25 anställda, med en andel om 40 procent.

Störst andel myndigheter som uppger att de *inte alls* eller *i låg grad* instämmer återfinns också hos de minsta myndigheterna med 23 procent. Hos de övriga myndighetskategorierna ligger andelen på 3-5 procent.

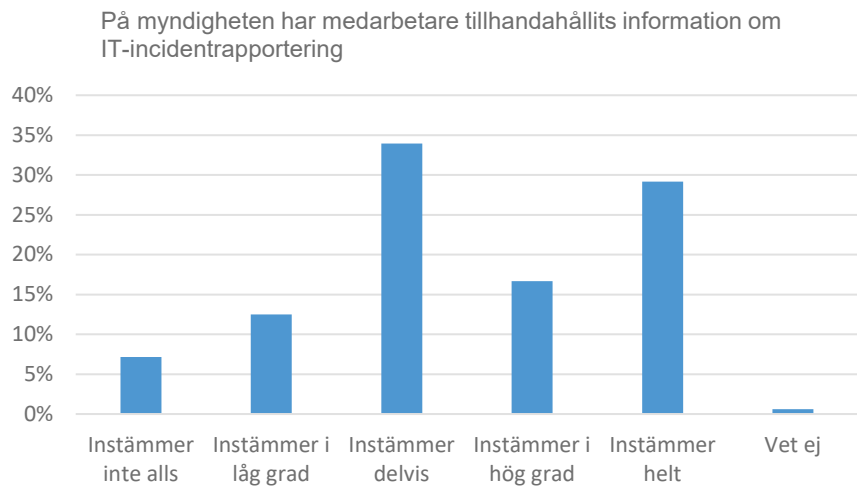


Figur 10: Fördelning av hur väl myndigheterna instämmer med att de har en rutin för att *rapportera* IT-incidenter grupperat efter myndighetskategorier.

B.2 Interna förutsättningar och förankring

B.2.1 Information till medarbetare om IT-incidentrapportering

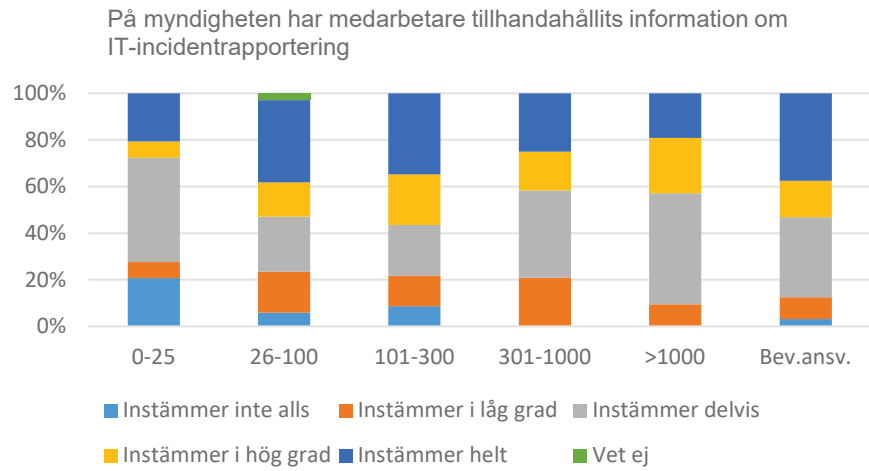
Bland samtliga myndigheter uppger 46 procent att de instämmer *i hög grad* eller *helt* i påståendet att medarbetare har tillhandahållits information om IT-incidentrapporteringen. Motsvarande andel för de som instämmer *i låg grad* eller *inte alls* är 20 procent.



Figur 11: Fördelning av hur väl myndigheterna instämmer med att medarbetare tillhandahållit information om IT-incidentrapportering.

Den största andelen som instämmer *i hög grad* eller *helt* återfinns i kategorin 101-300 anställda med 57 procent, följt av bevakningsansvariga myndigheter med 54 procent. Lägst andel myndigheter som instämmer *i hög grad* eller *helt* finns hos myndigheter med 0-25 anställda med en andel på 28 procent.

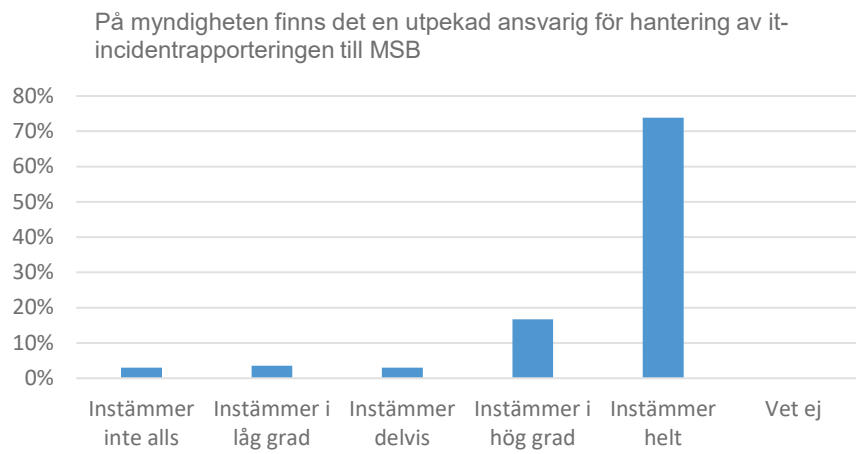
Andelen myndigheter som instämmer *i låg grad* eller *inte alls* i påståendet att medarbetare har tillhandahållits information om IT-incidentrapporteringen är relativt jämn över myndighetskategorierna. Bland de fyra första kategorierna (från 0-25 till 301-1000 anställda) uppmäter andelen till 21-28 procent. Hos myndigheter med fler än 1000 anställda samt bevakningsansvariga myndigheter är motsvarande spann 10-12 procent.



Figur 12: Fördelning av hur väl myndigheter instämmer med att medarbetare tillhandahållit information om IT-incidentrapportering grupperat efter myndighetskategorier.

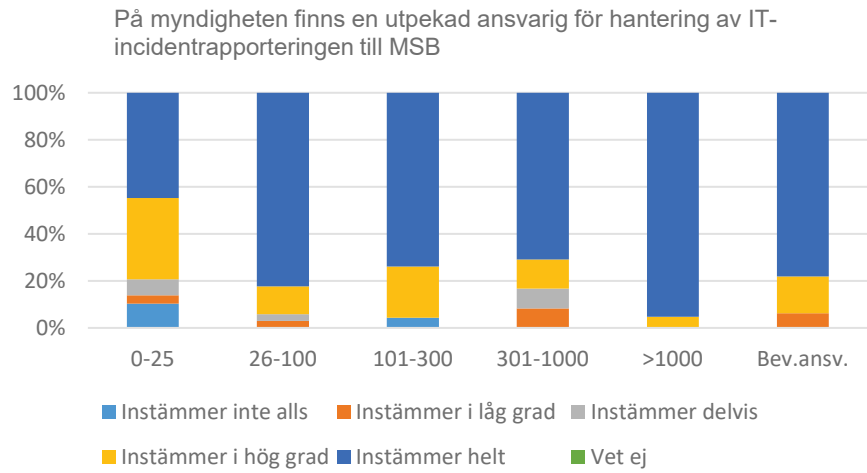
B.2.2 Utpekad ansvarig på myndigheten

Hos samtliga myndigheter är det 91 procent som uppger sig instämma *i hög grad* eller *helt* i påståendet att det finns en utpekad ansvarig för hantering av IT-incidenter på myndigheten. Motsvarande andel för dem som svarat *instämmer inte alls* eller *i låg grad* är 7 procent.



Figur 13: Fördelning av hur väl myndigheterna instämmer med att det finns en utpekad ansvarig för hantering av IT-incidentrapportering till MSB.

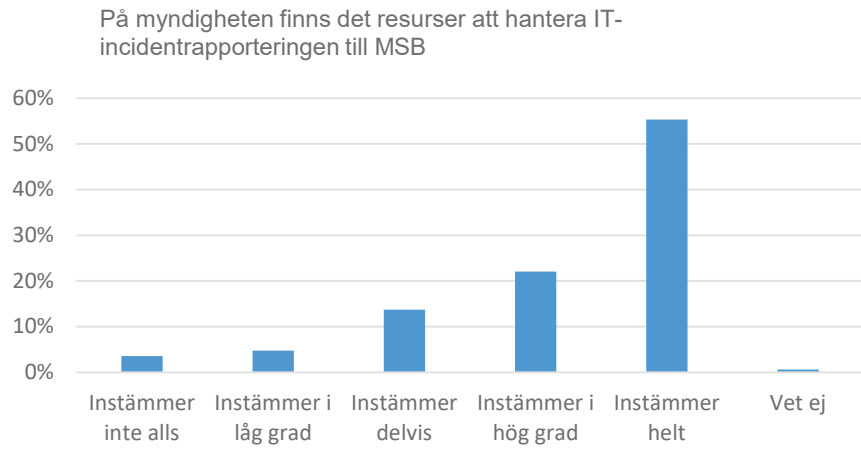
Andelen som uppger att de instämmer *i hög grad* eller *helt* är stor hos samtliga myndighetskategorier. Hos myndigheter med 0-25 anställda är andelen något lägre på 79 procent, hos de övriga ligger spannet på 84-100 procent. Andelen myndigheter som instämmer *i låg grad* eller *inte alls* i påståendet att det finns en utpekad ansvarig för hantering av IT-incidentrapportering är störst hos myndigheter med 0-25 anställda med 17 procent. Hos de övriga ligger spannet på 0-8 procent.



Figur 14: Fördelning av hur väl myndigheterna instämmer med att det finns en utpekad ansvarig för hantering av IT-incidentrapportering till MSB grupperat efter myndighetskategorier.

B.2.3 Resurser för IT-incidentrapportering

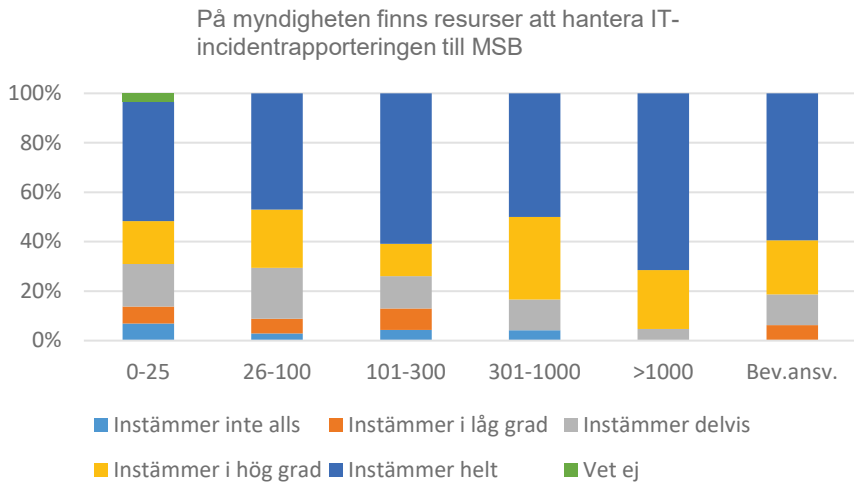
Andelen som instämmer *i hög grad* eller *helt* i påståendet att det finns resurser på myndigheten för att hantera rapporteringen av IT-incidenter uppgår till 77 procent. Motsvarande andel för dem som *instämmer i låg grad* eller *inte alls* är 9 procent.



Figur 15: Fördelning av hur väl myndigheterna instämmer med att det finns resurser att hantera rapporteringen av IT-incidenter till MSB.

Störst andel myndigheter som instämmer *i hög grad* eller *helt* finns bland dem med fler än 1000 anställda med en andel på 95 procent. Hos övriga kategorier ligger motsvarande andel på 65-81 procent, där de med 0-25 anställda svarar för den lägre andelen.

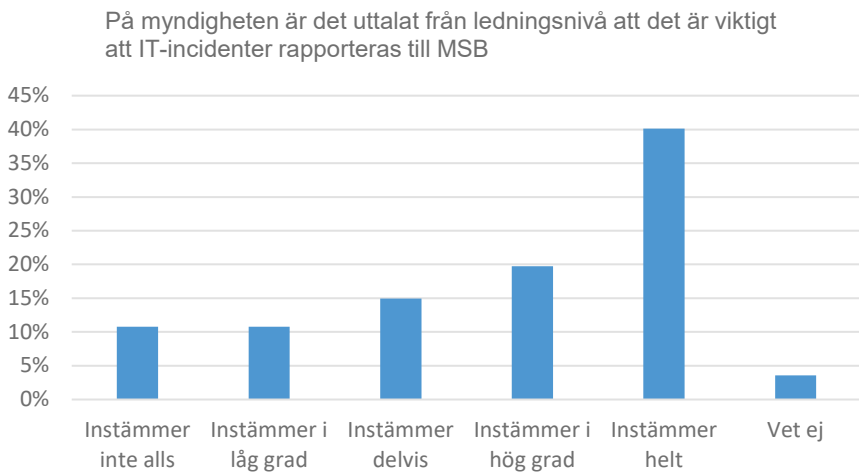
Störst andel myndigheter om angett att de instämmer *i låg grad* eller *inte alls* finns bland de med 0-25 anställda med 15 procent, följt av 101-300 anställda med 13 procent.



Figur 16: Fördelning av hur väl myndigheterna instämmer med att det finns resurser att hantera rapporteringen av IT-incidenter till MSB grupperat efter myndighetskategorier.

B.2.4 Uttalat stöd från ledningsnivå

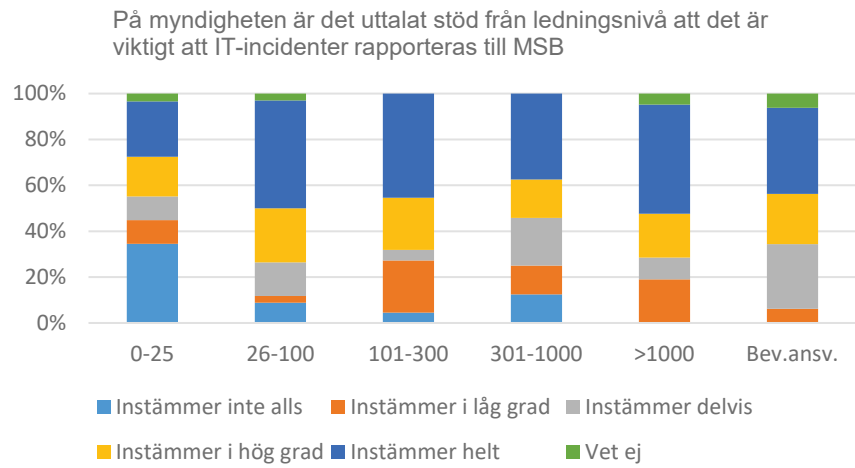
För samtliga myndigheter är det 60 procent som instämmer *i hög grad* eller *helt* att det finns ett uttalat stöd från ledningsnivå om att det är viktigt att IT-incidenter rapporteras till MSB. Motsvarande andel för de som instämmer *i låg grad* eller *inte alls* är 22 procent.



Figur 17: Fördelning av hur väl myndigheterna instämmer med att det är uttalat från ledningsnivå att det är viktigt att IT-incidenter rapporteras till MSB.

Myndigheter med 26-100 anställda har högst andel som svarat att de instämmer *i hög grad* eller *helt* med 71 procent. Därefter följer de med 101-300 anställda och fler än 1000 anställda med 68 respektive 67 procent. Lägst andel som instämmer *i hög grad* eller *helt* gällande uttalat stöd från ledningsnivå är myndigheter med 0-25 anställda med 41 procent, följt av de med 301-1000 anställda med 55 procent.

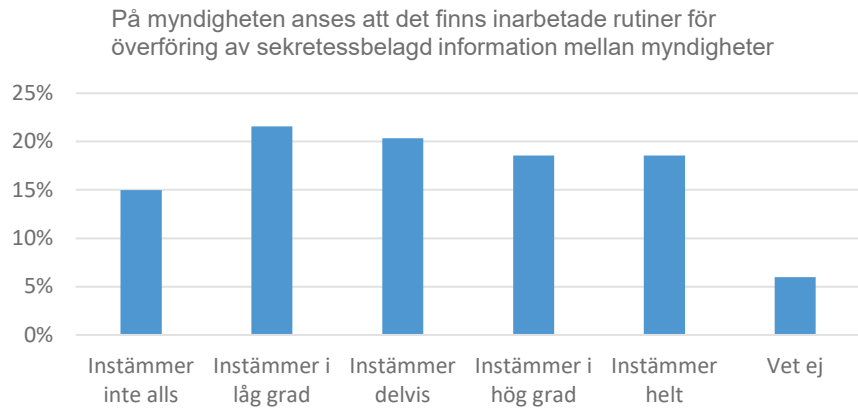
Bland myndigheterna som instämmer *i låg grad* eller *inte alls* återfinns störst andel bland myndigheter med 0-25 anställda. Hos dessa är andelen 44 procent. Hos övriga myndighetskategorier är spannet 6-28 procent där bevakningsansvariga myndigheter svarar för den lägre andelen och de med 101-300 anställda för den högre andelen.



Figur 18: Fördelning av hur väl myndigheterna instämmer med att det på myndigheten är uttalat från ledningsnivå att det är viktigt att IT-incidenter rapporteras till MSB, grupperat efter myndighetskategorier.

B.2.5 Rutiner för överföring av sekretessbelagd information

För samtliga myndigheter är det 38 procent som uppger att de instämmer *i hög grad* eller *helt* i påståendet att det finns inarbetade rutiner för överföring av sekretessbelagd information mellan myndigheter. Motsvarande siffra för andelen myndigheter som instämmer *i låg grad* eller *inte alls* är 37 procent.

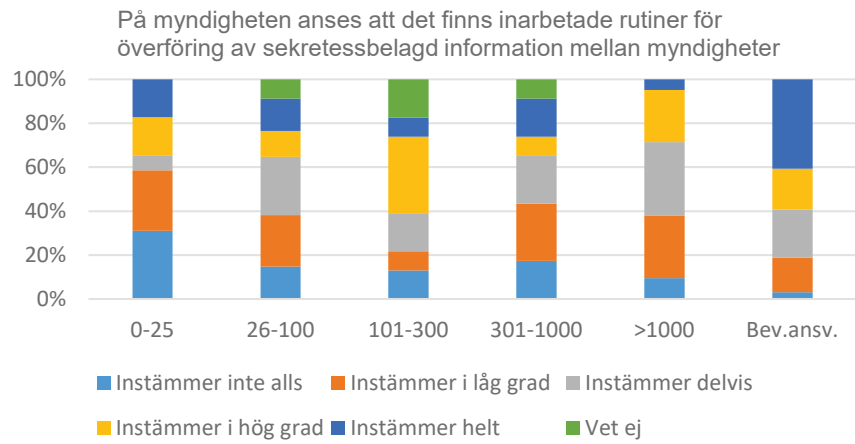


Figur 19: Fördelning av hur väl myndigheterna instämmer med att det finns rutiner för överföring av sekretessbelagd information.

Högst andel myndigheter som uppger att de instämmer *i hög grad* eller *helt* återfinns hos bevakningsansvariga myndigheter med en andel om 60 procent. Lägst andel står myndigheterna med 301-1000, 26-100, samt myndigheter med fler än 1000 anställda för med ett spann på mellan 26 och 29 procent.

De myndigheter som i störst utsträckning anger att de instämmer *i låg grad* eller *inte alls* är myndigheter med 0-25 anställda med en andel på 59 procent. Lägst andel återfinns bland bevakningsansvariga myndigheter och myndigheter med 101-300 anställda med 19 respektive 22 procent. För övriga myndigheter ligger spannet på mellan 39 och 43 procent.

Myndigheter som uppger att de *inte vet* huruvida det finns inarbetade rutiner för överföring av sekretessbelagd information mellan myndigheter återfinns i tre storlekskategorier. Störst andel återfinns hos myndigheter med 101-300 anställda med 17 procent. De två andra grupperna är de med 26-100 samt 301-1000 anställda där andelen hos dem båda uppgår till 9 procent.

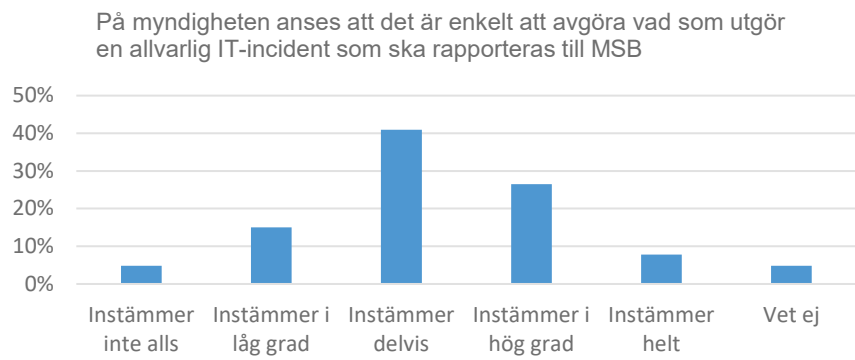


Figur 20: Fördelning av hur väl myndigheterna instämmer med att det finns rutiner för överföring av sekretessbelagd information grupperat efter myndighetskategorier.

B.3 Genomförande

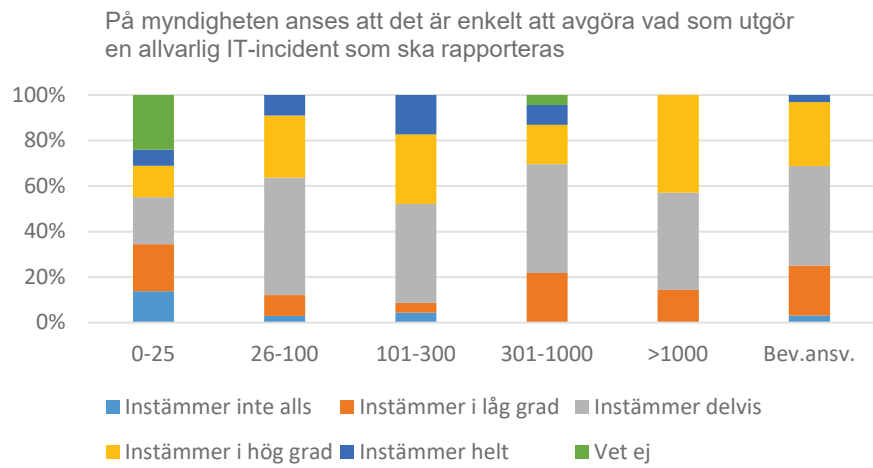
B.3.1 Enkelheten i att avgöra vad som utgör en allvarlig IT-incident

Enkätresultaten visar att 34 procent av de svarande myndigheterna instämmer *helt* eller *i hög grad* i påståendet att det är enkelt att avgöra vad som utgör en allvarlig IT-incident som ska rapporteras till MSB. Motsvarande procentsats för de myndigheter som *inte alls* eller *i låg grad* instämmer i påståendet är 20 procent.



Figur 21: Fördelning av hur väl myndigheterna instämmer med att det är enkelt att avgöra vad som utgör en allvarlig IT-incident som ska rapporteras till MSB.

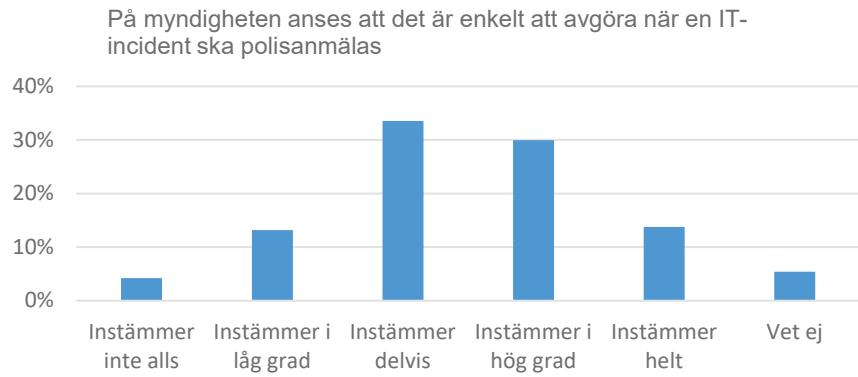
I vilken mån som myndigheterna håller med om påståendet att det är enkelt att avgöra om en IT-incident ska rapporteras varierar mellan storlekskategorierna. Störst andel myndigheter som instämmer *helt* eller *i hög grad* återfinns i kategorierna 101-300 samt fler än 1000 anställda med 48 respektive 43 procent. Lägst andel återfinns bland de mista myndigheterna (0-25 anställda) där sammantaget 21 procent instämmer *helt* eller *i hög grad*. Det är även bland de minsta myndigheterna som den största andelen av de som *inte alls* eller *i låg grad* instämmer i påståendet (34 procent).



Figur 22: Fördelning av hur väl myndigheterna instämmer med att det är enkelt att avgöra vad som utgör en allvarlig IT-incident som ska rapporteras till MSB grupperat efter myndighetskategorier.

B.3.2 Enkelheten i att avgöra om en IT-incident ska polisanmälas

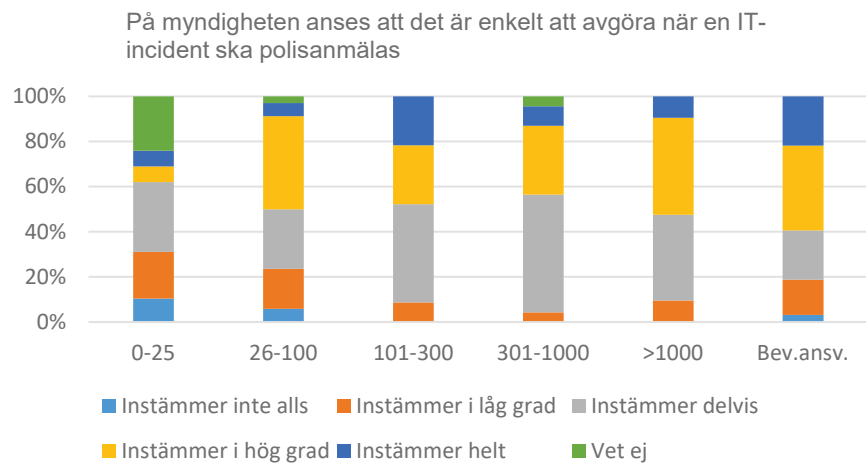
Sammantaget svarar 44 procent av myndigheterna att de *helt* eller *i hög grad* håller med om påståendet att det är enkelt att avgöra när en IT-incident ska polisanmälas. Motsvarande 17 procent uppger att de *inte alls* eller *i låg grad* instämmer.



Figur 23: Fördelning av hur väl myndigheterna instämmer med att det är enkelt att avgöra när en IT-incident ska polisanmälas.

Bevakningsansvariga myndigheter är den kategori med störst andel (59 procent) som *helt* eller *i hög grad* instämmer i påståendet om att det är enkelt att avgöra om en IT-incident ska polisanmälas. Lägst andel, med 14 procent, återfinns bland de minsta myndigheterna med 0-25 anställda.

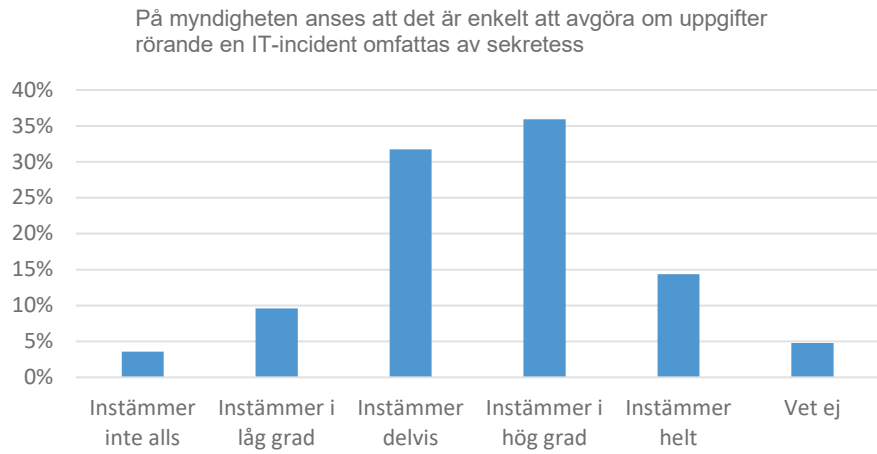
De minsta myndigheterna är de som i störst utsträckning *inte alls* eller *i låg grad* håller med om påståendet, med en andel om 31 procent. Därefter följer kategorierna 26-100 anställda med 24 procent och bevakningsansvariga myndigheter med 19 procent.



Figur 24: Fördelning av hur väl myndigheterna instämmer med att det är enkelt att avgöra när en IT-incident ska polisanmälas grupperat efter myndighetskategorier.

B.3.3 Enkelheten i att avgöra om uppgifter rörande en IT-incident omfattas av sekretess

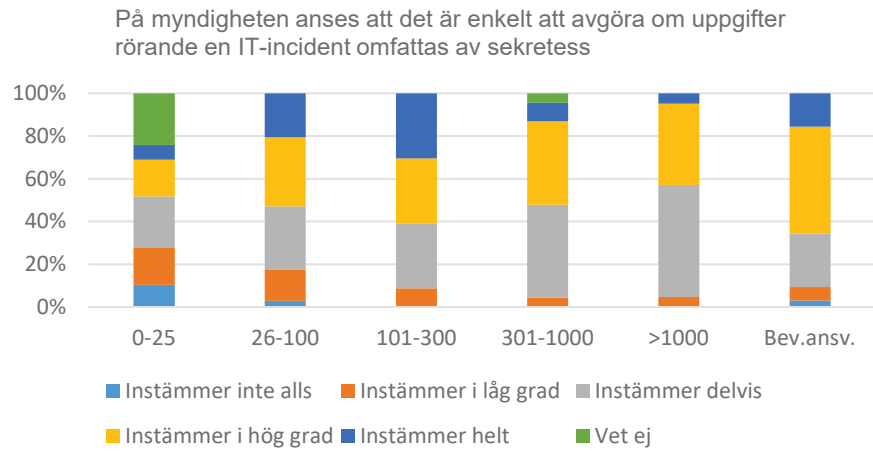
På frågan om myndigheten anser att det är enkelt att avgöra om uppgifter rörande en IT-incident omfattas av sekretess uppgav 50 procent av myndigheterna att de *helt* eller *i hög grad* instämmer. Motsvarande 13 procent uppgav att de inte alls eller i låg grad instämmer med påståendet.



Figur 25: Fördelning av hur väl myndigheterna instämmer med att det är enkelt att avgöra om uppgifter rörande en IT-incident omfattas av sekretess.

Bland myndigheter som *helt* eller *i hög grad* instämmer i påståendet återfinns störst andel bland bevakningsansvariga myndigheter (med 66 procent) och myndigheter med 101-300 anställda (med 61 procent). Lägst andel, med 24 procent, återfinns bland myndigheter med 0-25 anställda.

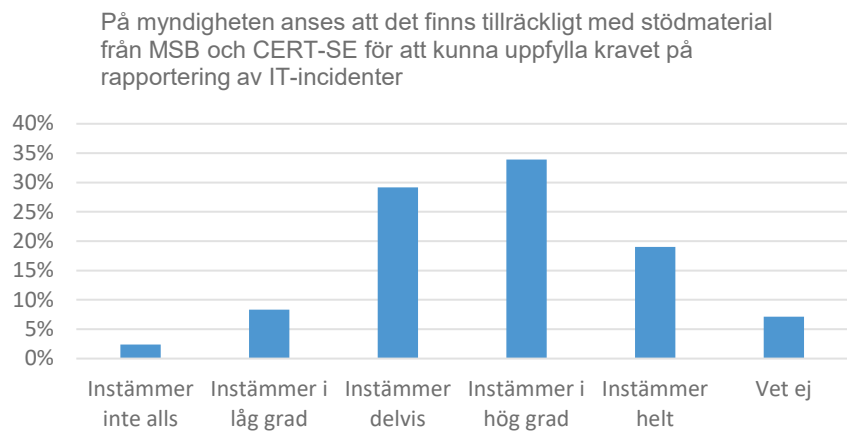
De minsta myndigheterna är också de som i störst utsträckning *inte alls* eller *i låg grad* håller med om påståendet, med en andel om 28 procent. Lägst andel myndigheter som inte håller med påståendet återfinns bland myndigheterna i storlekskategorierna 301-1000 och fler än 1000 anställda med 4 respektive 5 procent.



Figur 26: Fördelning av hur väl myndigheterna instämmer med att det är enkelt att avgöra om uppgifter rörande en IT-incident omfattas av sekretess grupperat efter myndighetskategorier.

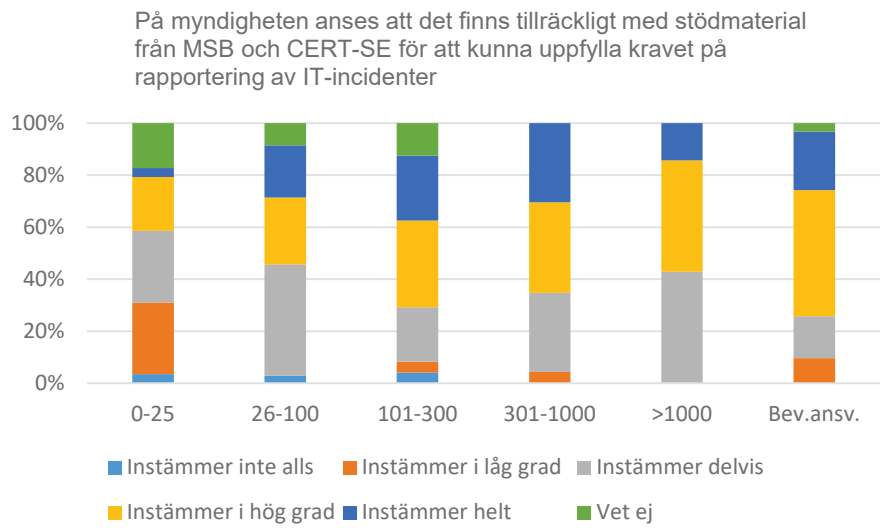
B.3.4 Stödmaterial från MSB och CERT-SE

Enkätresultaten visar att 53 procent av de svarande myndigheterna instämmer *helt* eller *i hög grad* i påståendet att det finns tillräckligt med stödmaterial från MSB och CERT-SE för att myndigheterna ska kunna uppfylla kravet på IT-incidentrapportering. Motsvarande procentsats för de myndigheter som *inte alls* eller *i låg grad* instämmer i påståendet är 11 procent.



Figur 27: Fördelning av hur väl myndigheterna instämmer med att det finns tillräckligt med stödmaterial från MSB och CERT-SE.

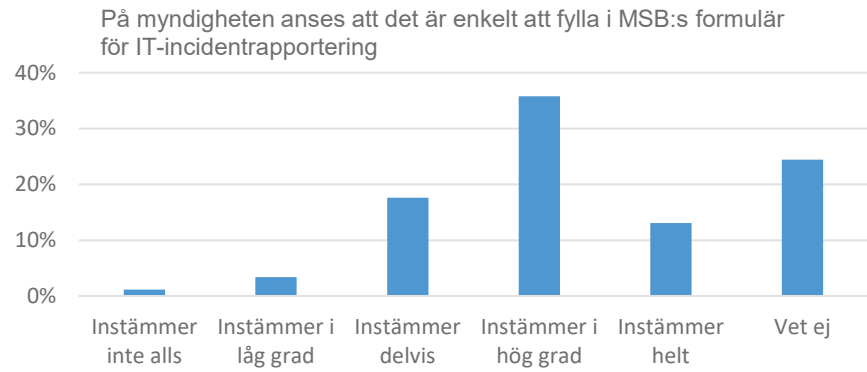
De myndigheter som i enkätundersökningen i störst utsträckning *helt* eller *i hög grad* instämmer i påståendet är bevakningsansvariga samt myndigheter med 301-1000 anställda, med andelar om 71 respektive 65 procent. I kategorin 0-25 anställda är andelen som lägst, med 24 procent. Samma storlekskategori, 0-25 anställda, har därutöver störst andel myndigheter, 31 procent, som *inte alls* eller *i låg grad* håller med i påståendet samt störst andel som svarat *Vet ej* (17 procent).



Figur 28: Fördelning av hur väl myndigheterna instämmer med att det finns tillräckligt med stödmaterial från MSB och CERT-SE grupperat efter myndighetskategorier.

B.3.5 Enkelheten i att fylla i MSB:s formulär för rapportering av IT-incidenter

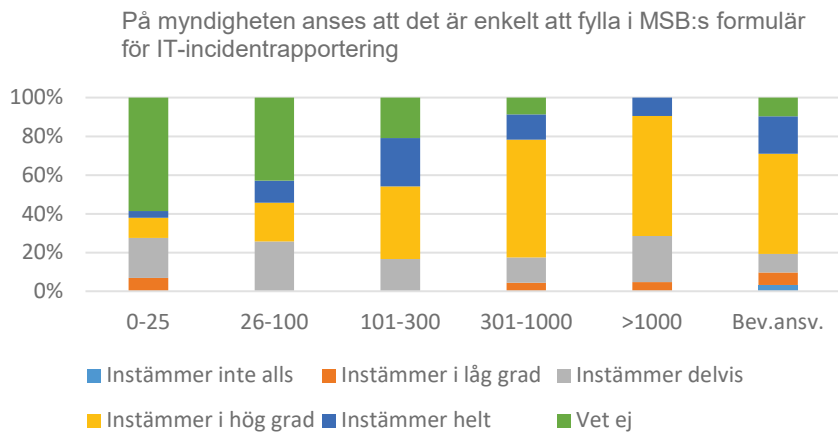
Enkätresultaten visar att 49 procent av de svarande myndigheterna instämmer *helt* eller *i hög grad* i påståendet att det är enkelt att fylla i MSB:s formulär för IT-incidentrapportering. Motsvarande procentsats för de myndigheter som *inte alls* eller *i låg grad* instämmer i påståendet är 5 procent. Sammantaget svarar också 24 procent av myndigheterna att de *inte vet*.



Figur 29: Fördelning av hur väl myndigheterna instämmer med att det är enkelt att fylla i MSB:s formulär för IT-incidentrapportering.

Störst andel myndigheter som *helt* eller *i hög grad* instämmer i påståendet återfinns bland de tre myndighetskategorier som alla har fler än 300 anställda. Andelen för dessa kategorier varierar mellan 71 och 74 procent. Minst andel har kategorin 0-25 anställda med en andel om 14 procent.

Störst andel myndigheter som svarat att de *inte alls* eller *i låg grad* håller med i påståendet återfinns bland bevakningsansvariga myndigheter med en andel om 10 procent. Andelen i respektive kategori som svarat *vet ej* på påståendet varierar kraftigt, från 59 procent för myndigheter med 0-25 anställda till 0 procent för myndigheter med fler än 1000 anställda.

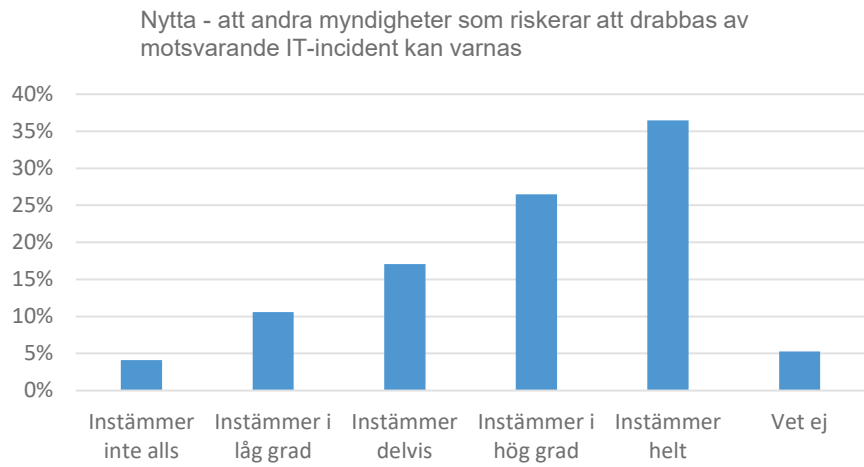


Figur 30: Fördelning av hur väl myndigheterna instämmer med att det är enkelt att fylla i MSB:s formulär för IT-incidentrapportering grupperat efter myndighetskategorier.

B.4 Upplevd nytta

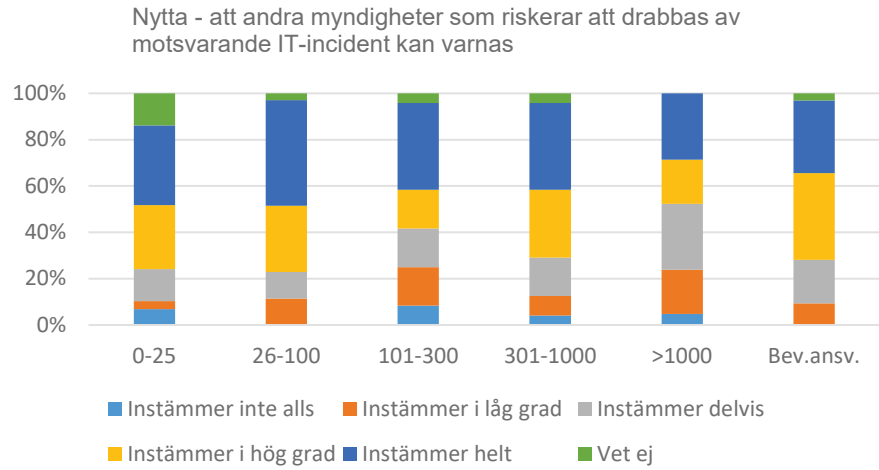
B.4.1 Att andra myndigheter som riskerar att drabbas av motsvarande IT-incident kan varnas

På frågan om myndigheten upplevde att en nytta med IT-incidentrapporteringen till MSB är att andra myndigheter som riskerar att drabbas av motsvarande IT-incident kan varnas instämde sammantaget 63 procent av myndigheterna *helt* eller *i hög grad*. Motsvarande 15 procent svarade att de *inte alls* eller *i låg grad* instämde.



Figur 31: Fördelning av hur väl myndigheterna instämmer med att nyttan med att rapportera IT-incidenter är att andra myndigheter som riskerar att drabbas av motsvarande incident kan varnas.

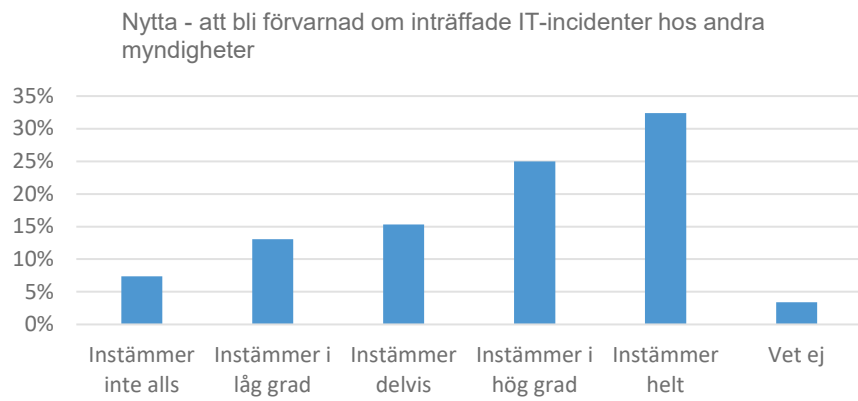
Myndigheter med 26-100 anställda samt bevakningsansvariga myndigheter är de kategorier med störst andel myndigheter som svarat att de instämmer *helt* eller *i hög grad* (74 respektive 69 procent). Lägst andel har myndigheter med fler än 1000 anställda samt 101-300 anställda (48 respektive 54 procent). Dessa två storlekskategorier har därutöver störst andel myndigheter som *inte alls* eller *i låg grad* instämmer med frågan (24 respektive 25 procent).



Figur 32: Fördelning av hur väl myndigheterna instämmer med att nyttan med att rapportera IT-incidenter är att andra myndigheter som riskerar att drabbas av motsvarande incident kan varnas, fördelat efter myndighetskategori.

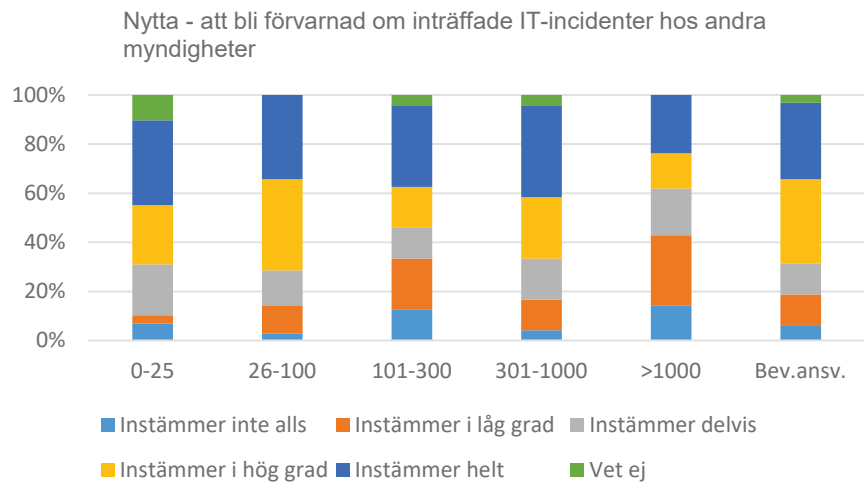
B.4.2 Att bli förvarnad om inträffade IT-incidenter hos andra myndigheter

Sammantaget svarar 57 procent av myndigheterna att de *helt* eller *i hög grad* håller med om att en nytta med IT-incidentrapporteringen är att bli förvarnad om inträffade IT-incidenter hos andra myndigheter. Motsvarande 20 procent uppger att de *inte alls* eller *i låg grad* instämmer.



Figur 33: Fördelning av hur väl myndigheterna instämmer med att nyttan med att rapportera IT-incidenter är att bli förvarnad om inträffade IT-incidenter hos andra myndigheter.

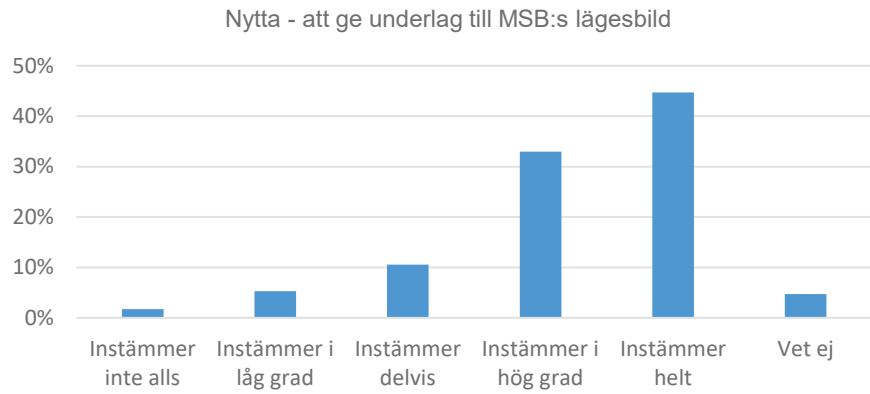
De myndigheter som i enkätundersökningen i störst utsträckning *helt* eller *i hög grad* instämmer om nyttan med rapporteringen är myndigheter med 26-100 anställda, med en andel om 71 procent. I kategorin fler än 1000 anställda är andelen som lägst, med 38 procent. Samma storlekskategori, fler än 1000 anställda, har därutöver störst andel myndigheter, 43 procent, som *inte alls* eller *i låg grad* instämmer om den förvarnande nyttan med rapporteringen. Motsvarande lägst andel återfinns bland de minsta myndigheterna, 0-25 anställda, med 10 procent.



Figur 34: Fördelning av hur väl myndigheterna instämmer med att nyttan med att rapportera IT-incidenter är att bli förvarnad om inträffade IT-incidenter hos andra myndigheter, grupperat efter myndighetskategorier.

B.4.3 Att ge underlag till MSB:s lägesbild

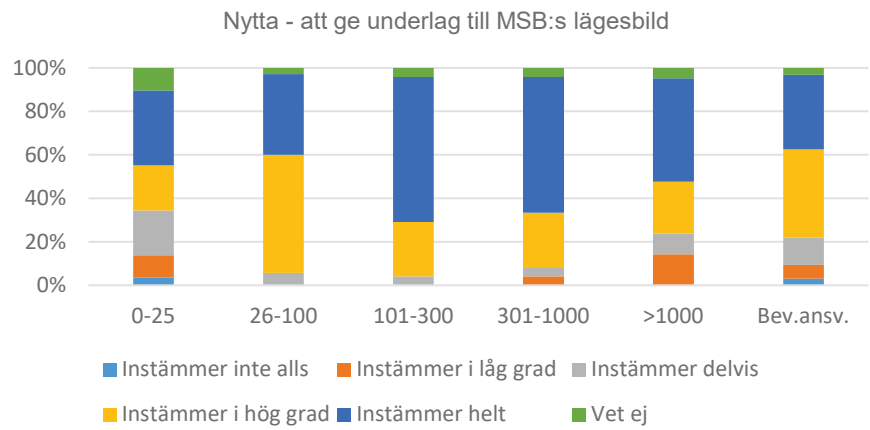
Enkätresultaten visar att 78 procent av de svarande myndigheterna instämmer *helt* eller *i hög grad* i att en nytta med IT-incidentrapporteringen är att ge underlag till MSB:s lägesbild. Motsvarande procentsats för de myndigheter som *inte alls* eller *i låg grad* instämmer om nyttan är 7 procent.



Figur 35: Fördelning av hur väl myndigheterna instämmer med att nyttan med att rapportera IT-incidenter är att ge underlag till MSB:s lägesbild.

Störst andel myndigheter som *helt* eller *i hög grad* instämmer om nyttan med rapporteringen återfinns bland de tre mellersta myndighetskategorierna, det vill säga myndigheter med 26-1000 anställda. Andelen för dessa kategorier varierar mellan 88 och 92 procent. Minst andel har kategorin 0-25 anställda med en andel om 55 procent.

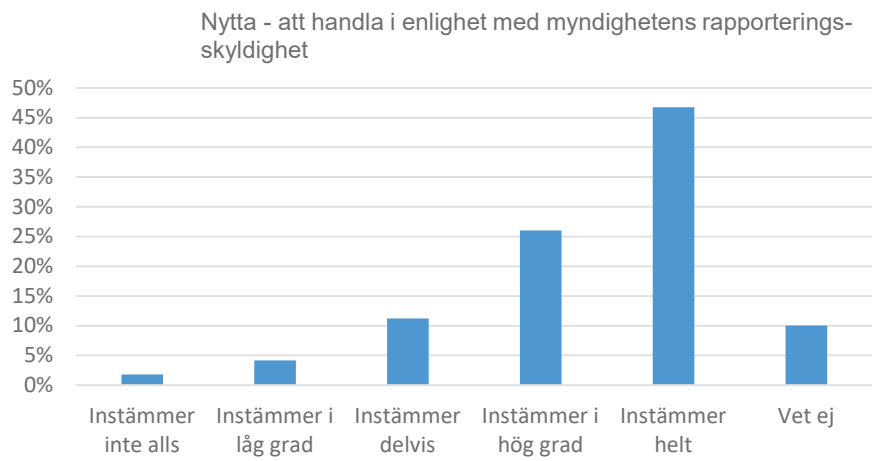
Störst andel myndigheter som svarat att de *inte alls* eller *i låg grad* håller med i påståendet återfinns bland de minsta myndigheterna samt myndigheter med fler än 1000 anställda, med en andel om 14 procent.



Figur 36: Fördelning av hur väl myndigheterna instämmer med att nyttan med att rapportera IT-incidenter är att ge underlag till MSB:s lägesbild, grupperat efter myndighetskategori.

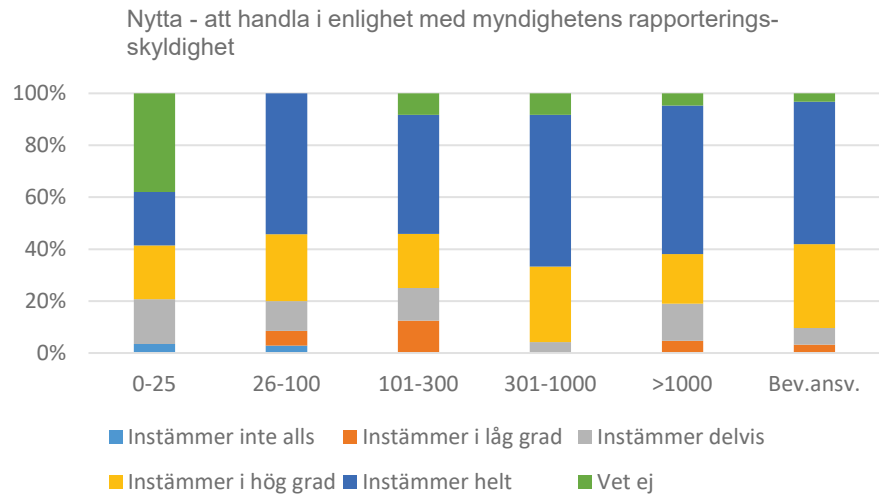
B.4.4 Att handla i enlighet med myndighetens rapporteringsskyldighet

Sammantaget svarar 73 procent av myndigheterna att de *helt* eller *i hög grad* håller med om att en nytta med IT-incidentrapporteringen är att handla i enlighet het myndighetens rapporteringsskyldighet. Motsvarande 6 procent uppger att de *inte alls* eller *i låg grad* instämmer.



Figur 37: Fördelning av hur väl myndigheterna instämmer med att nyttan med att rapportera IT-incidenter är att handla i enlighet med myndighetens rapporteringsskyldighet.

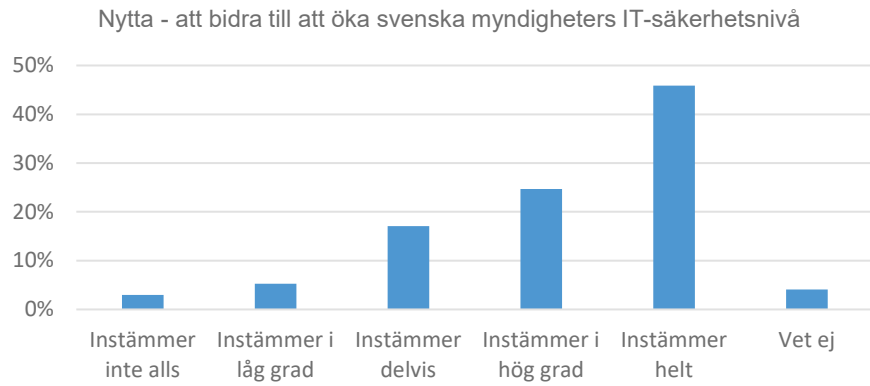
Myndigheter med 301-100 anställda samt bevakningsansvariga myndigheter är de kategorier med störst andel myndigheter som svarat att de instämmer *helt* eller *i hög grad* (88 respektive 87 procent). Lägst andel har myndigheter med 0-25 anställda med 41 procent. Myndigheter med 101-300 anställda har störst andel myndigheter som *inte alls* eller *i låg grad* instämmer med nyttan (13 procent). Tilläggas bör att 38 procent av de allra minsta myndigheterna har svarat *vet ej* på frågan.



Figur 38: Fördelning av hur väl myndigheterna instämmer med att nyttan med att rapportera IT-incidenter är att handla i enlighet med myndighetens rapporteringsskyldighet, grupperat efter myndighetskategori.

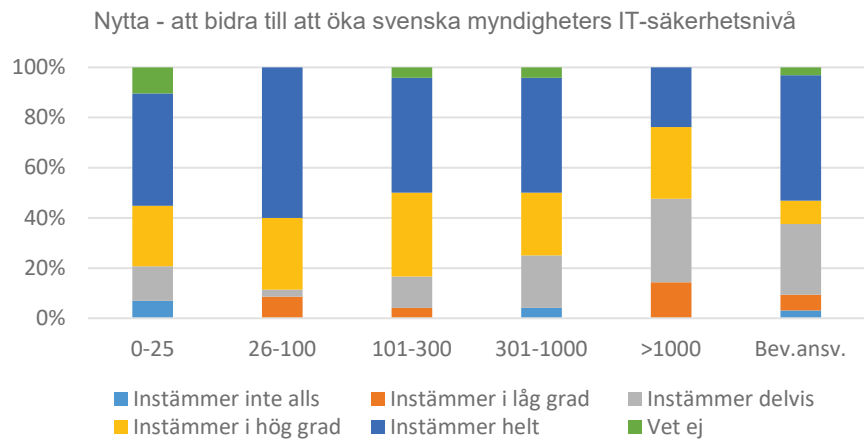
B.4.5 Att bidra till att öka svenska myndigheters IT-säkerhetsnivå

På frågan om myndigheten upplevde att en nytta med IT-incidentrapporteringen till MSB är att bidra till att öka svenska myndigheters IT-säkerhetsnivå instämde sammantaget 71 procent av myndigheterna *helt* eller *i hög grad*. Motsvarande 8 procent svarade att de *inte alls* eller *i låg grad* instämde.



Figur 39: Fördelning av hur väl myndigheterna instämmer med att nyttan med att rapportera IT-incidenter är att bidra till att öka svenska myndigheters IT-säkerhetsnivå.

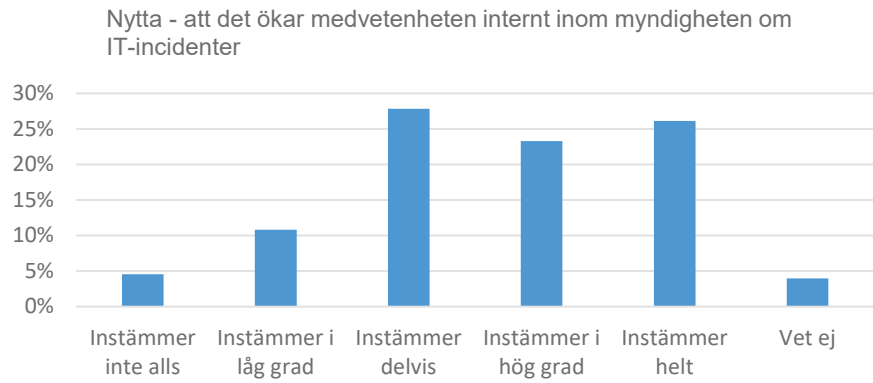
De myndigheter som i enkätundersökningen i störst utsträckning *helt* eller *i hög grad* instämmer om nyttan med rapporteringen är myndigheter med 26-100 anställda, med en andel om 89 procent. I kategorin fler än 1000 anställda är andelen som lägst, med 52 procent. Samma storlekskategori, fler än 1000 anställda, har därutöver störst andel myndigheter, 14 procent, som *inte alls* eller *i låg grad* instämmer om den förvarnande nyttan med rapporteringen. Motsvarande lägst andel återfinns bland myndigheter med 26-100 samt 101-300 anställda, båda med en andel om 4 procent.



Figur 40: Fördelning av hur väl myndigheterna instämmer med att nyttan med att rapportera IT-incidenter är att bidra till att öka svenska myndigheters IT-säkerhetsnivå, grupperat efter myndighetskategori.

B.4.6 Att det ökar medvetenheten internt inom myndigheten om IT-incidenter

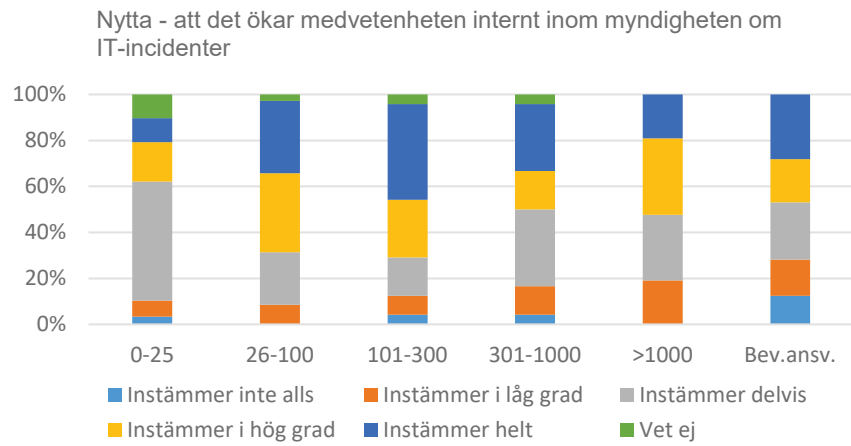
Enkätresultaten visar att 49 procent av de svarande myndigheterna instämmer *helt* eller *i hög grad* i att en nytta med IT-incidentrapporteringen är att det bidrar till att öka medvetenheten internt inom myndigheten om IT-incidenter. Motsvarande procentsats för de myndigheter som *inte alls* eller *i låg grad* instämmer är 15 procent.



Figur 41: Fördelning av hur väl myndigheterna instämmer med att nyttan med att rapportera IT-incidenter är att det ökar medvetenheten internt inom myndigheten om IT-incidenter.

Störst andel myndigheter som *helt* eller *i hög grad* instämmer om nyttan med rapporteringen återfinns bland myndigheter med 26-100 samt 101-300 anställda (med 66 respektive 67 procent). Minst andel har kategorin 0-25 anställda med en andel om 28 procent.

Störst andel myndigheter som svarat att de *inte alls* eller *i låg grad* håller med i påståendet återfinns bland de bevakningsansvariga myndigheterna, med en andel om 28 procent.



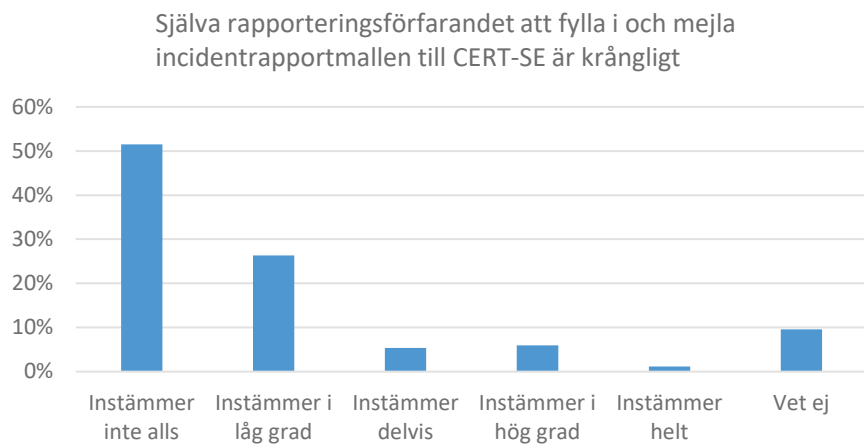
Figur 42: Fördelning av hur väl myndigheterna instämmer med att nyttan med att rapportera IT-incidenter är att det ökar medvetenheten internt inom myndigheten om IT-incidenter, grupperat efter myndighetskategorier.

B.5 Hypotetiskt scenario – Utebliven rapportering

I avsnitten som följer presenteras resultaten från det hypotetiska scenario som berör rapportering av IT-incidenter till MSB. Scenariot utgörs av tolv påståenden som respondenten bedömer var för sig avseende i vilken utsträckning påståendet skulle kunna utgöra anledning till att rapportering av IT-incident inte sker till MSB.

B.5.1 Krångligt rapporteringsförfarande

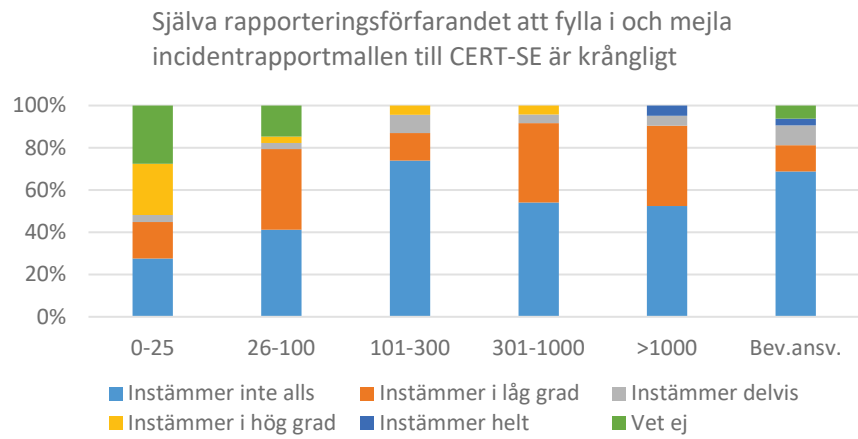
Bland samtliga myndigheter uppger 7 procent att de instämmer *i hög grad* eller *helt* med påståendet att *själva rapporteringsförfarandet att fylla i och mejla incidentrapportmallen till CERT-SE är krångligt* skulle kunna vara en anledning till att rapportering av IT-incident till MSB inte sker. Motsvarande andel som instämmer *i låg grad* eller *inte alls* är 78 procent.



Figur 43: Fördelning av hur väl myndigheterna instämmer med påståendet om att ett krångligt rapporteringsförfarande kan vara anledning till att IT-incidentrapportering uteblir.

Den största andelen som instämmer *i hög grad* eller *helt* med påståendet återfinns i kategorin 0-25 anställda med 24 procent, följt av kategorin fler än 1000 anställda med 5 procent.

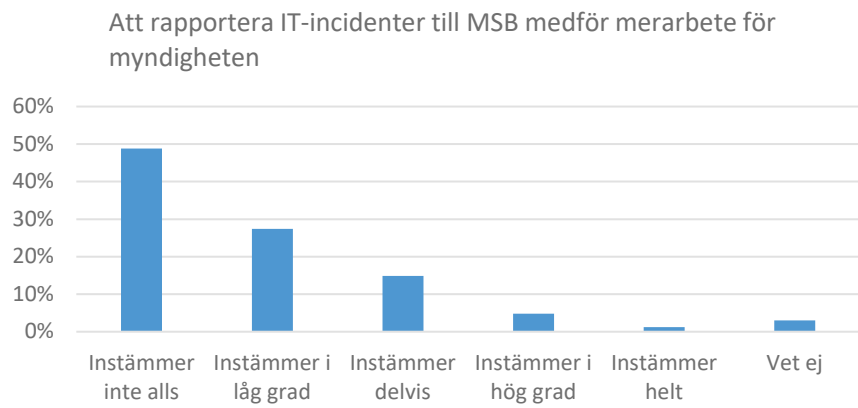
Den största andelen som instämmer *i låg grad* eller *inte alls* med att påståendet skulle kunna vara en anledning till att rapportering av IT-incident till MSB inte sker återfinns i kategorin 301-1000 anställda med 92 procent, följt av kategorin fler än 1000 anställda med 90 procent.



Figur 44: Fördelning av hur väl myndigheterna instämmer med påståendet om att ett krångligt rapporteringsförfarande kan vara anledning till att IT-incidentrapportering uteblir, grupperat efter myndighetskategorier.

B.5.2 Merarbete för myndigheten

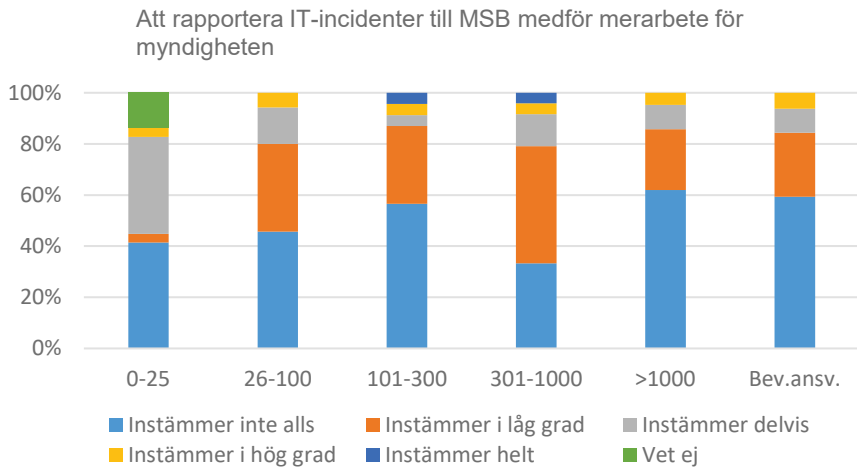
Bland samtliga myndigheter uppger 6 procent att de instämmer *i hög grad* eller *helt* med påståendet *att rapportera IT-incidenter till MSB medför merarbete för myndigheten* skulle kunna vara en anledning till att rapportering av IT-incident till MSB inte sker. Motsvarande siffra för andelen som instämmer *i låg grad* eller *inte alls* är 76 procent.



Figur 45: Fördelning av hur väl myndigheterna instämmer med påståendet om att ett medfört merarbete med IT-incidentrapporteringen kan vara anledning till att IT-incidentrapportering uteblir.

Den största andelen som instämmer *i hög grad* eller *helt* med att påståendet skulle kunna vara en anledning till att rapportering av IT-incident till MSB inte sker återfinns i kategorin 101-300 anställda med 9 procent, följt av kategorin 301-1000 anställda med 8 procent.

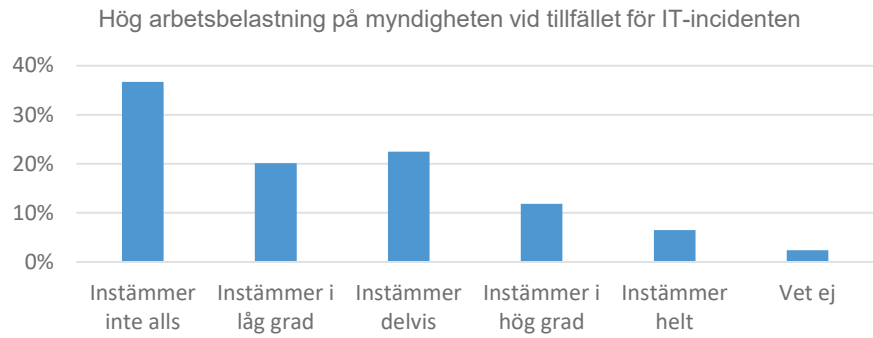
Den största andelen som instämmer *i låg grad* eller *inte alls* med påståendet återfinns i kategorin 101-300 anställda med 87 procent, följt av kategorin fler än 1000 anställda med 86 procent.



Figur 46: Fördelning av hur väl myndigheterna instämmer med påståendet om att ett medfört merarbete med IT-incidentrapporteringen kan vara anledning till att IT-incidentrapportering uteblir, grupperat efter myndighetskategorier.

B.5.3 Hög arbetsbelastning på myndigheten

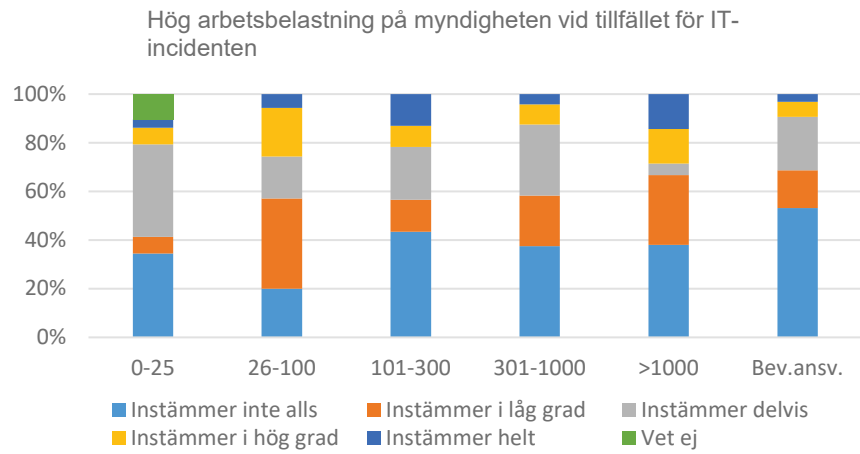
Bland samtliga myndigheter uppger 18 procent att de instämmer *i hög grad* eller *helt* med påståendet *hög arbetsbelastning på myndigheten vid tillfället för IT-incidenten* skulle kunna vara en anledning till att rapportering av IT-incident till MSB inte sker. Motsvarande siffra för andelen som instämmer *i låg grad* eller *inte alls* är 57 procent.



Figur 47: Fördelning av hur väl myndigheterna instämmer med påståendet om att hög arbetsbelastning på myndigheten vid tillfället för en IT-incident kan vara anledning till att IT-incidentrapportering uteblir.

Den största andelen som instämmer *i hög grad* eller *helt* med att påståendet skulle kunna vara en anledning till att rapportering av IT-incident till MSB inte sker återfinns i kategorin fler än 1000 anställda med 29 procent, följt av kategorin 26-100 anställda med 26 procent.

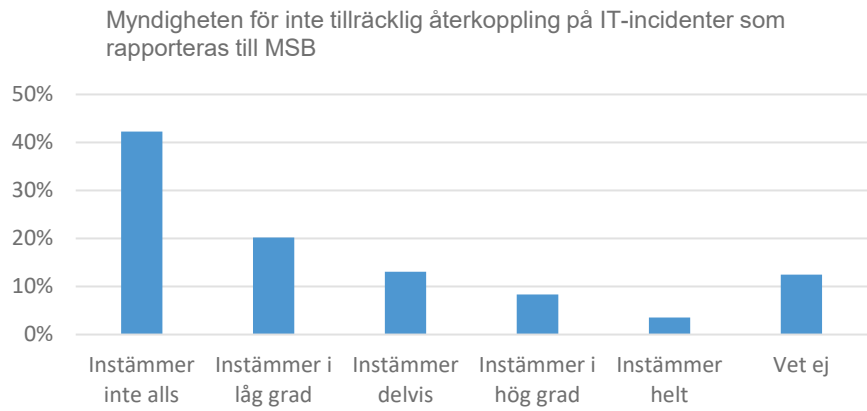
Den största andelen som instämmer *i låg grad* eller *inte alls* med påståendet återfinns i kategorin bevakningsansvariga myndigheter med 69 procent, följt av kategorin fler än 1000 anställda med 67 procent.



Figur 48: Fördelning av hur väl myndigheterna instämmer med påståendet om att hög arbetsbelastning på myndigheten vid tillfället för en IT-incident kan vara anledning till att IT-incidentrapportering uteblir, grupperat efter myndighetskategorier.

B.5.4 Otillräcklig återkoppling

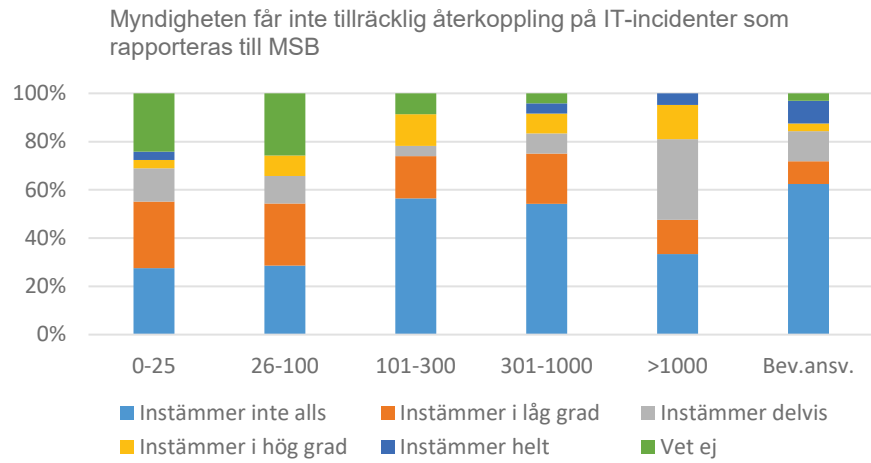
Bland samtliga myndigheter uppger 12 procent att de instämmer *i hög grad* eller *helt* med påståendet *myndigheten får inte tillräcklig återkoppling på IT-incidenter som rapporteras till MSB* som möjlig anledning till att rapportering av IT-incident till MSB inte sker. Motsvarande siffra för andelen som instämmer *i låg grad* eller *inte alls* är 63 procent.



Figur 49: Fördelning av hur väl myndigheterna instämmer med påståendet om att otillräcklig återkoppling från MSB på rapporterade IT-incidenter kan vara anledning till att IT-incidentrapportering uteblir.

Den största andelen som instämmer *i hög grad* eller *helt* med påståendet återfinns i kategorin fler än 1000 anställda med 19 procent, följt av kategorin 101-300 anställda med 13 procent.

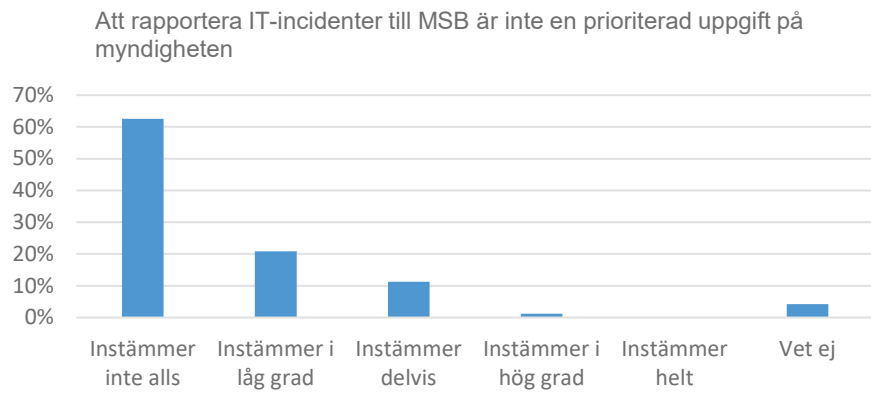
Den största andelen som instämmer *i låg grad* eller *inte alls* med att påståendet skulle kunna vara en anledning till att rapportering av IT-incident till MSB inte sker återfinns i kategorin 301-1000 anställda med 75 procent, följt av kategorin 101-300 anställda med 74 procent.



Figur 50: Fördelning av hur väl myndigheterna instämmer med påståendet om att otillräcklig återkoppling från MSB på rapporterade IT-incidenter kan vara anledning till att IT-incidentrapportering uteblir, grupperat efter myndighetskategorier.

B.5.5 Ej prioriterad uppgift

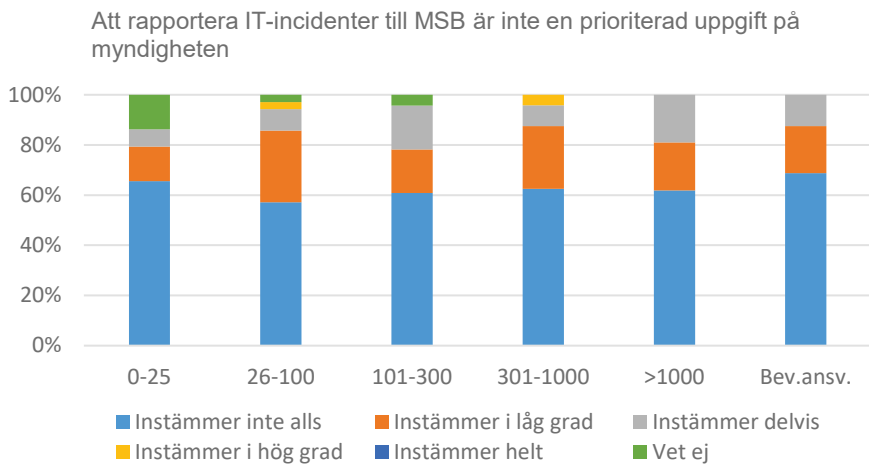
Bland samtliga myndigheter uppger 1 procent att de instämmer *i hög grad* eller *helt* med påståendet *att rapportera IT-incidenter till MSB är inte en prioriterad uppgift på myndigheten* skulle kunna vara en anledning till att rapportering av IT-incident till MSB inte sker. Motsvarande siffra för andelen som instämmer *i låg grad* eller *inte alls* är 83 procent.



Figur 51: Fördelning av hur väl myndigheterna instämmer med påståendet om att IT-incidentrapporteringen inte betraktas som en prioriterad uppgift vid myndigheten som anledning till att IT-incidentrapportering uteblir.

Den största andelen som instämmer *i hög grad* eller *helt* med påståendet återfinns i kategorin 301-1000 anställda med 4 procent, följt av kategorin 26-100 anställda med 3 procent.

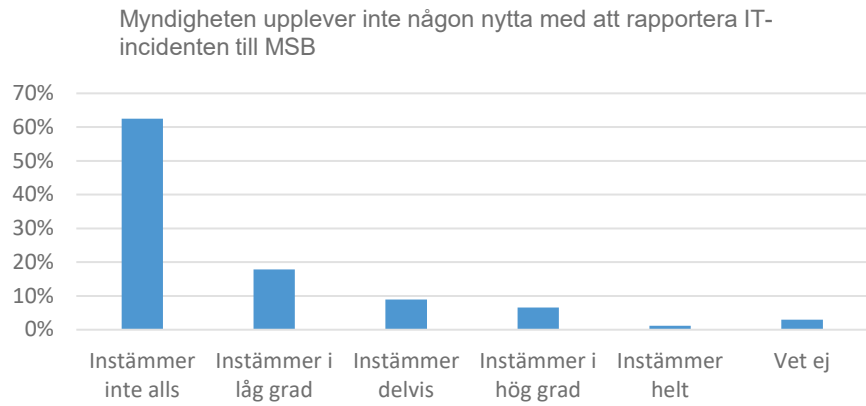
Den största andelen som instämmer *i låg grad* eller *inte alls* med att påståendet skulle kunna vara en anledning till att rapportering av IT-incident till MSB inte sker återfinns i kategorierna 301-1000 anställda samt bevakningsansvariga myndigheter, båda med 88 procent.



Figur 52: Fördelning av hur väl myndigheterna instämmer med påståendet om att IT-incidentrapporteringen inte betraktas som en prioriterad uppgift vid myndigheten som anledning till att IT-incidentrapportering uteblir, grupperat efter myndighetskategorier.

B.5.6 Ingen upplevd nytta

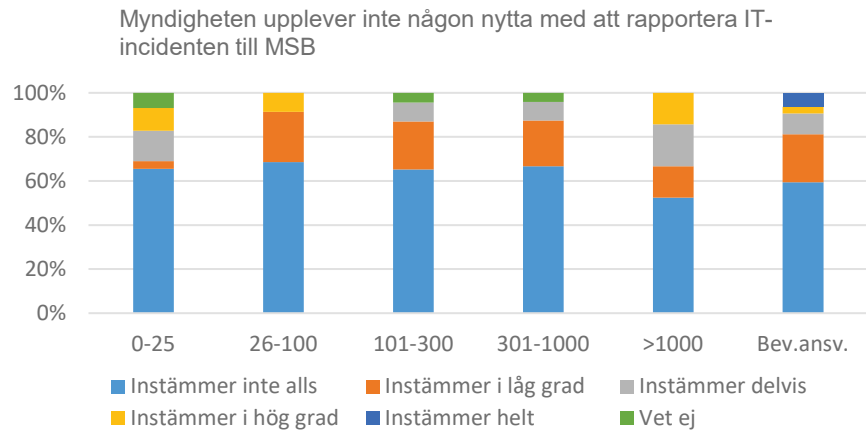
Bland samtliga myndigheter uppger 8 procent att de instämmer *i hög grad* eller *helt* med påståendet *myndigheten upplever inte någon nytta med att rapportera IT-incidenter till MSB* som möjlig anledning till att rapportering av IT-incident till MSB inte sker. Motsvarande siffra för andelen som instämmer *i låg grad* eller *inte alls* är 80 procent.



Figur 53: Fördelning av hur väl myndigheterna instämmer med påståendet om att oupplevd nytta med IT-incidentrapporteringen kan vara anledning till att IT-incidentrapportering uteblir.

Den största andelen som instämmer *i hög grad* eller *helt* med påståendet återfinns i kategorin fler än 1000 anställda med 14 procent, följt av kategorin 0-25 anställda med 10 procent.

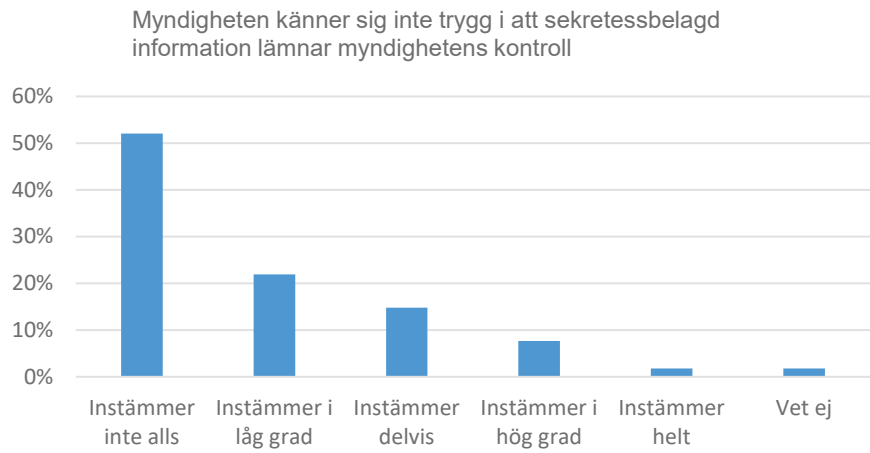
Den största andelen som instämmer *i låg grad* eller *inte alls* med att påståendet skulle kunna vara en anledning till att rapportering av IT-incident till MSB inte sker återfinns i kategorin 26-100 anställda med 91 procent, följt av kategorin 301-1000 anställda med 88 procent.



Figur 54: Fördelning av hur väl myndigheterna instämmer med påståendet om att oupplevd nytta med IT-incidentrapporteringen kan vara anledning till att IT-incidentrapportering uteblir, grupperat efter myndighetskategorier.

B.5.7 Hantering av sekretessbelagd information

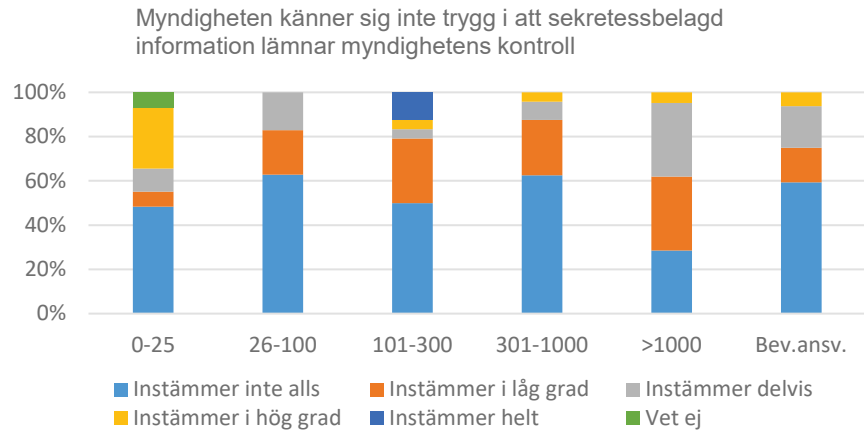
Bland samtliga myndigheter uppger 9 procent att de instämmer *i hög grad* eller *helt* med påståendet *myndigheten känner sig inte trygg i att sekretessbelagd information lämnar myndighetens kontroll* som möjlig anledning till att rapportering av IT-incident till MSB inte sker. Motsvarande siffra för andelen som instämmer *i låg grad* eller *inte alls* är 74 procent.



Figur 55: Fördelning av hur väl myndigheterna instämmer med påståendet om att en otrygghet i att sekretessbelagd information lämnar myndighetens kontroll kan vara anledning till att IT-incidentrapportering uteblir.

Den största andelen som instämmer *i hög grad* eller *helt* med påståendet återfinns i kategorin 0-25 anställda med 28 procent, följt av kategorin 101-300 anställda med 17 procent.

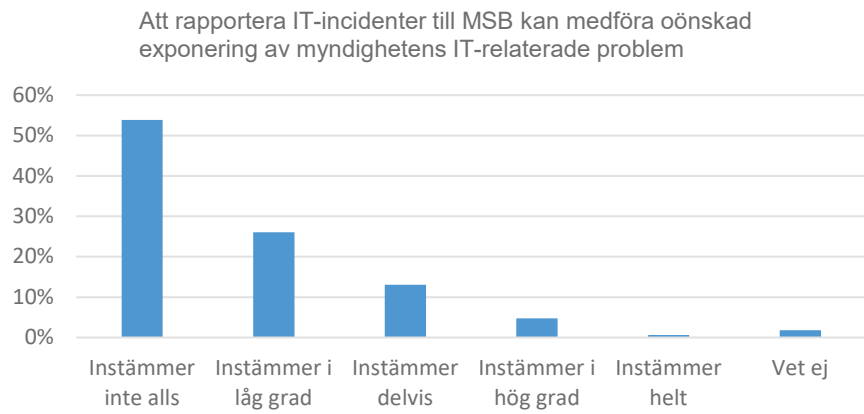
Den största andelen som instämmer *i låg grad* eller *inte alls* med att påståendet skulle kunna vara en anledning till att rapportering av IT-incident till MSB inte sker återfinns i kategorin 301-1000 anställda med 88 procent, följt av kategorin 26-100 anställda med 83 procent.



Figur 56: Fördelning av hur väl myndigheterna instämmer med påståendet om att en otrygghet i att sekretessbelagd information lämnar myndighetens kontroll kan vara anledning till att IT-incidentrapportering uteblir, grupperat efter myndighetskategorier.

B.5.8 Oönskad exponering

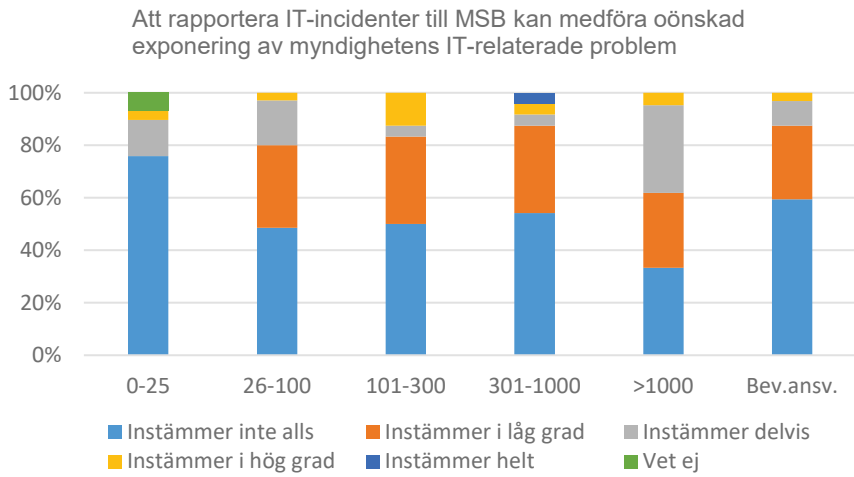
Bland samtliga myndigheter uppger 5 procent att de instämmer *i hög grad* eller *helt* med påståendet *att rapportera IT-incidenter till MSB kan medföra oönskad exponering av myndighetens IT-relaterade problem* skulle kunna vara en anledning till att rapportering av IT-incident till MSB inte sker. Motsvarande siffra för andelen som instämmer *i låg grad* eller *inte alls* är 80 procent.



Figur 57: Fördelning av hur väl myndigheterna instämmer med påståendet om att en medförd exponering av myndighetens IT-relaterade problem kan vara anledning till att IT-incidentrapportering uteblir.

Den största andelen som instämmer *i hög grad* eller *helt* med att påståendet skulle kunna vara en anledning till att rapportering av IT-incident till MSB inte sker återfinns i kategorin 101-300 anställda med 13 procent, följt av kategorin 301-1000 anställda med 8 procent.

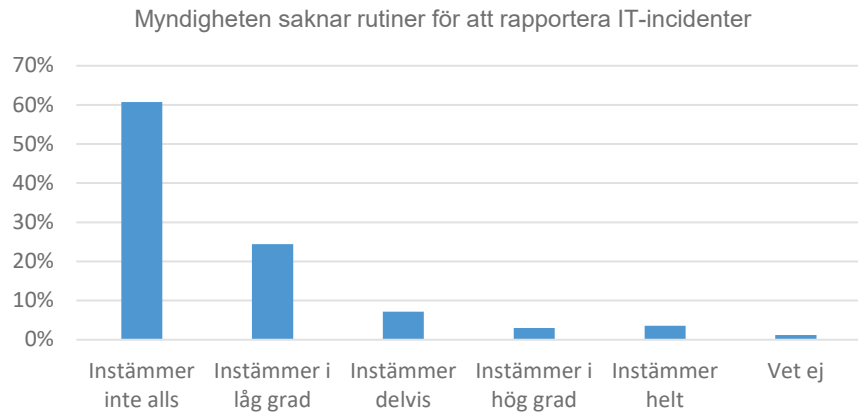
Den största andelen som instämmer *i låg grad* eller *inte alls* med påståendet återfinns i kategorierna 301-1000 anställda samt bevakningsansvariga myndigheter, båda med 88 procent.



Figur 58: Fördelning av hur väl myndigheterna instämmer med påståendet om att en medförd exponering av myndighetens IT-relaterade problem kan vara anledning till att IT-incidentrapportering uteblir, grupperat efter myndighetskategorier.

B.5.9 Rutiner saknas

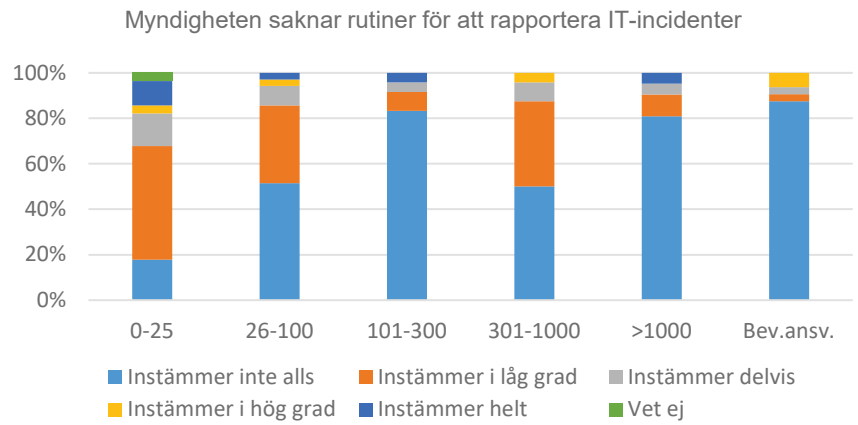
Bland samtliga myndigheter uppger 7 procent att de instämmer *i hög grad* eller *helt* med påståendet att *myndigheten saknar rutiner för att rapportera IT-incidenter* skulle kunna vara en anledning till att rapportering av IT-incident till MSB inte sker. Motsvarande siffra för andelen som instämmer *i låg grad* eller *inte alls* är 85 procent.



Figur 59: Fördelning av hur väl myndigheterna instämmer med påståendet om att en avsaknad av rutiner för IT-incidentrapportering kan vara anledning till att IT-incidentrapportering uteblir.

Den största andelen som instämmer *i hög grad* eller *helt* med påståendet återfinns i kategorin 0-25 anställda med 14 procent, följt av kategorin bevakningsansvariga myndigheter med 6 procent.

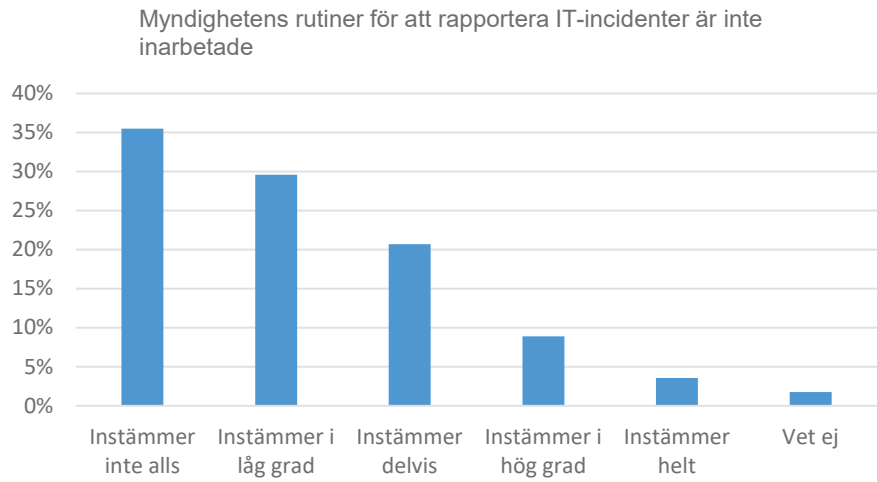
Den största andelen som instämmer *i låg grad* eller *inte alls* med att påståendet skulle kunna vara en anledning till att rapportering av IT-incident till MSB inte sker återfinns i kategorin 101-300 anställda med 92 procent, följt av kategorin bevakningsansvariga myndigheter med 91 procent.



Figur 60: Fördelning av hur väl myndigheterna instämmer med påståendet om att en avsaknad av rutiner för IT-incidentrapportering kan vara anledning till att IT-incidentrapportering uteblir, grupperat efter myndighetskategorier.

B.5.10 Ej inarbetade rutiner

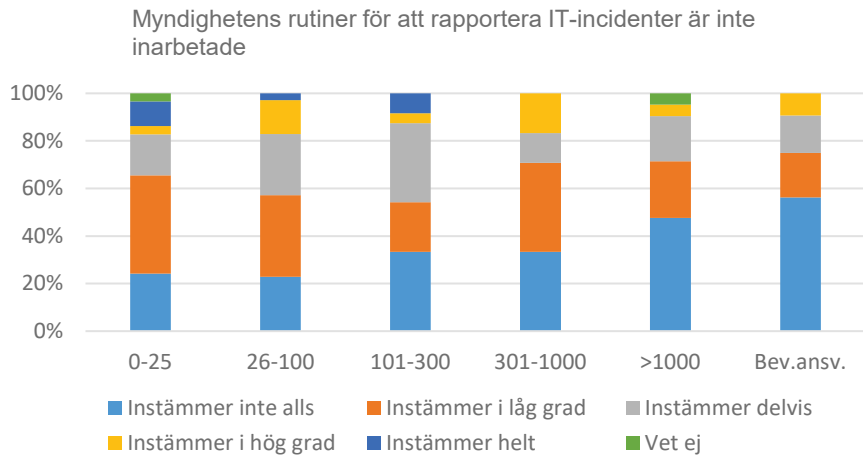
Bland samtliga myndigheter uppger 12 procent att de instämmer *i hög grad* eller *helt* med påståendet att *myndighetens rutiner för att rapportera IT-incidenter är inte inarbetade* skulle kunna vara en anledning till att rapportering av IT-incident till MSB inte sker. Motsvarande siffra för andelen som instämmer *i låg grad* eller *inte alls* är 65 procent.



Figur 61: Fördelning av hur väl myndigheterna instämmer med påståendet om att icke inarbetade rutiner för IT-incidentrapportering kan vara anledning till att IT-incidentrapportering uteblir.

Den största andelen som instämmer *i hög grad* eller *helt* med påståendet återfinns i kategorierna 26-100 anställda samt 301-1000 anställda, båda med 17 procent.

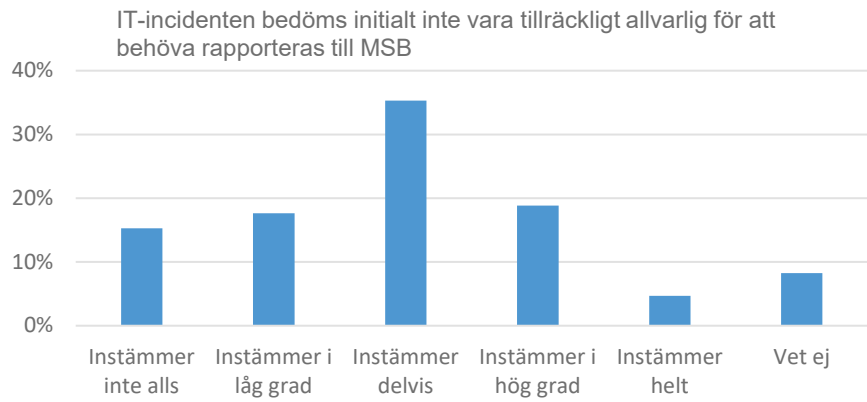
Den största andelen som instämmer *i låg grad* eller *inte alls* med påståendet återfinns i kategorin bevakningsansvariga myndigheter med 75 procent, följt av kategorierna 301-1000 anställda samt fler än 1000 anställda, båda med 71 procent.



Figur 62: Fördelning av hur väl myndigheterna instämmer med påståendet om att icke inarbetade rutiner för IT-incidentrapportering kan vara anledning till att IT-incidentrapportering uteblir, grupperat efter myndighetskategorier.

B.5.11 Initialt inte tillräckligt allvarlig

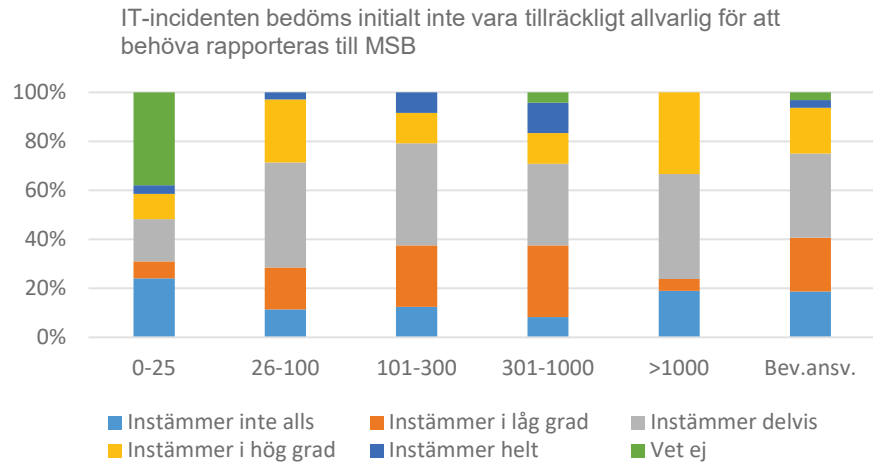
Bland samtliga myndigheter uppger 24 procent att de instämmer *i hög grad* eller *helt* med påståendet att *IT-incidenten bedöms initialt inte vara tillräckligt allvarlig för att behöva rapporteras till MSB* skulle kunna vara en anledning till att rapportering av IT-incident till MSB inte sker. Motsvarande siffra för andelen som instämmer *i låg grad* eller *inte alls* är 33 procent.



Figur 63: Fördelning av hur väl myndigheterna instämmer med påståendet om att en initial bedömning att IT-incidenten inte är tillräckligt allvarlig kan vara anledning till att IT-incidentrapportering uteblir.

Den största andelen som instämmer *i hög grad* eller *helt* med att påståendet skulle kunna vara en anledning till att rapportering av IT-incident till MSB inte sker återfinns i kategorin fler än 1000 anställda med 33 procent, följt av kategorin 26-100 anställda med 29 procent.

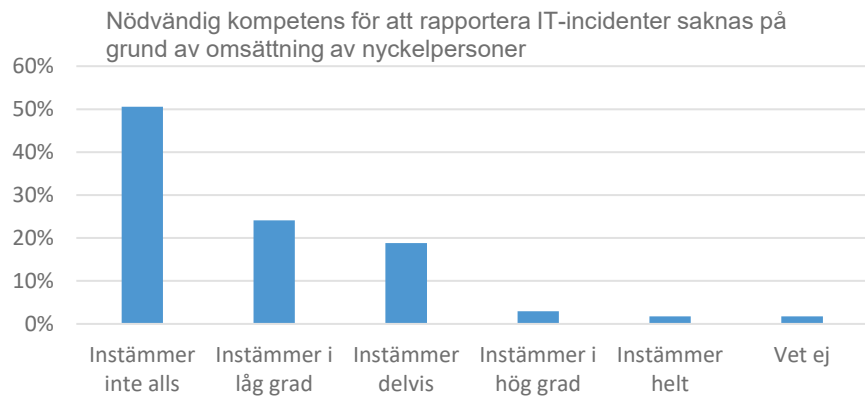
Den största andelen som instämmer *i låg grad* eller *inte alls* med att påståendet skulle kunna vara en anledning till att rapportering av IT-incident till MSB inte sker återfinns i kategorin bevakningsansvariga myndigheter med 41 procent, följt av kategorierna 101-300 anställda samt 310-1000 anställda, båda med 38 procent.



Figur 64: Fördelning av hur väl myndigheterna instämmer med påståendet om att en initial bedömning att IT-incidenten inte är tillräckligt allvarlig kan vara anledning till att IT-incident-rapportering uteblir, grupperat efter myndighetskategorier.

B.5.12 Omsättning av nyckelpersoner

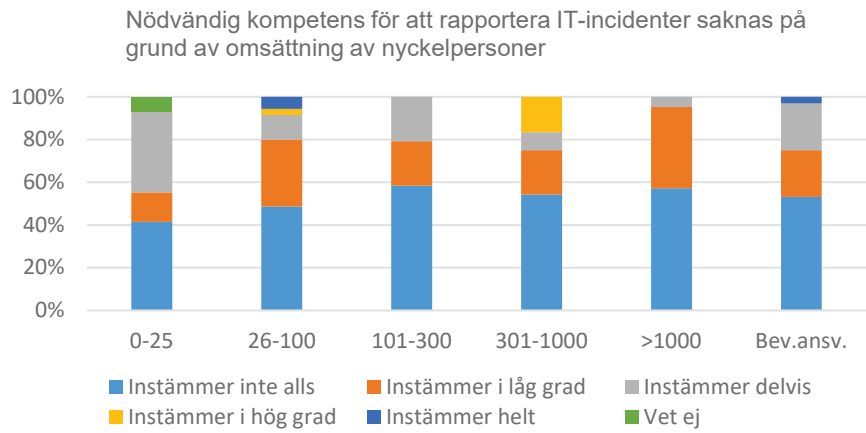
Bland samtliga myndigheter uppger 5 procent att de instämmer *i hög grad* eller *helt* med påståendet att *nödvändig kompetens för att rapportera IT-incidenter saknas på grund av omsättning av nyckelpersoner* skulle kunna vara en anledning till att rapportering av IT-incident till MSB inte sker. Motsvarande siffra för andelen som instämmer *i låg grad* eller *inte alls* är 75 procent.



Figur 65: Fördelning av hur väl myndigheterna instämmer med påståendet om att avsaknad av nödvändig kompetens på grund av personalomsättning av kan vara anledning till att IT-incidentrapportering uteblir.

Den största andelen som instämmer *i hög grad* eller *helt* med påståendet återfinns i kategorin 301-1000 anställda med 17 procent, följt av kategorin 26-100 anställda med 9 procent.

Den största andelen som instämmer *i låg grad* eller *inte alls* med att påståendet skulle kunna vara en anledning till att rapportering av IT-incident till MSB inte sker återfinns i kategorin fler än 1000 anställda med 95 procent, följt av kategorin 26-100 anställda med 80 procent.



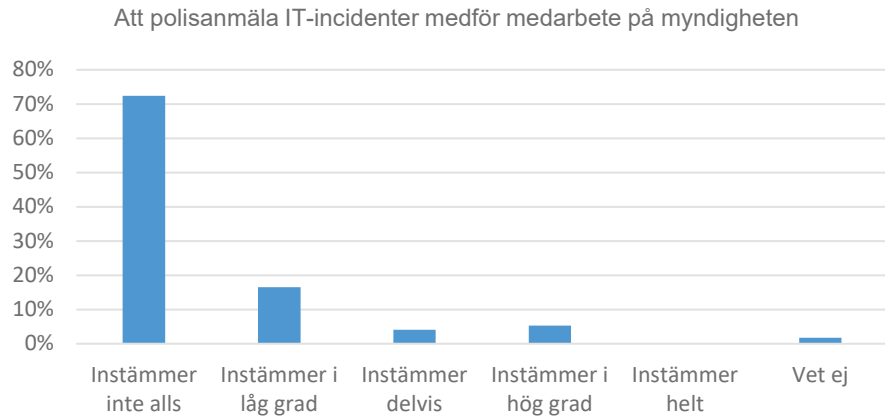
Figur 66: Fördelning av hur väl myndigheterna instämmer med påståendet om att avsaknad av nödvändig kompetens på grund av personalomsättning av kan vara anledning till att IT-incidentrapportering uteblir, grupperat efter myndighetskategorier.

B.6 Hypotetiskt scenario – Utebliven polisanmälan

I avsnitten som följer presenteras resultaten från det hypotetiska scenariot som berör polisanmälan av IT-incidenter. Scenariot utgörs av nio påståenden som respondenten bedömer var för sig avseende i vilken utsträckning påståendet skulle kunna utgöra anledning till att polisanmälan av IT-incident inte sker.

B.6.1 Merarbete på myndigheten

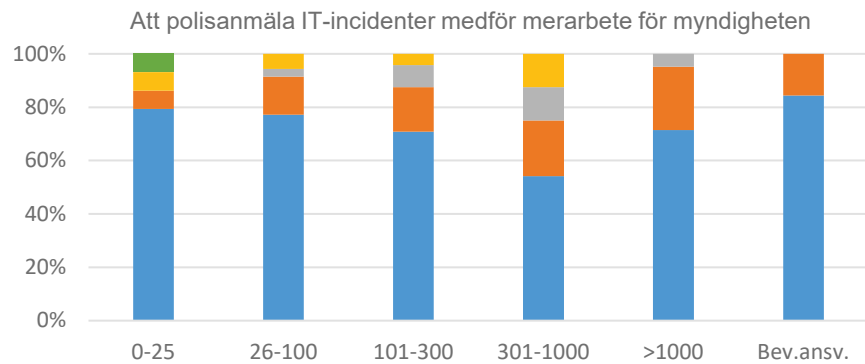
Bland samtliga myndigheter uppger 5 procent att de instämmer *i hög grad* eller *helt* med påståendet *att polisanmäla IT-incidenter medför merarbete för myndigheten* skulle kunna vara en anledning till att polisanmälan av IT-incident inte sker. Motsvarande siffra för andelen som instämmer *i låg grad* eller *inte alls* är 89 procent.



Figur 67: Fördelning av hur väl myndigheterna instämmer med påståendet om att ett medfört merarbete med polisanmälan av en IT-incident kan vara anledning till att polisanmälan uteblir.

Den största andelen som instämmer *i hög grad* eller *helt* med att påståendet skulle kunna vara en anledning till att polisanmälan av IT-incident inte sker återfinns i kategorin 301-1000 anställda med 13 procent, följt av kategorin 0-25 anställda med 7 procent.

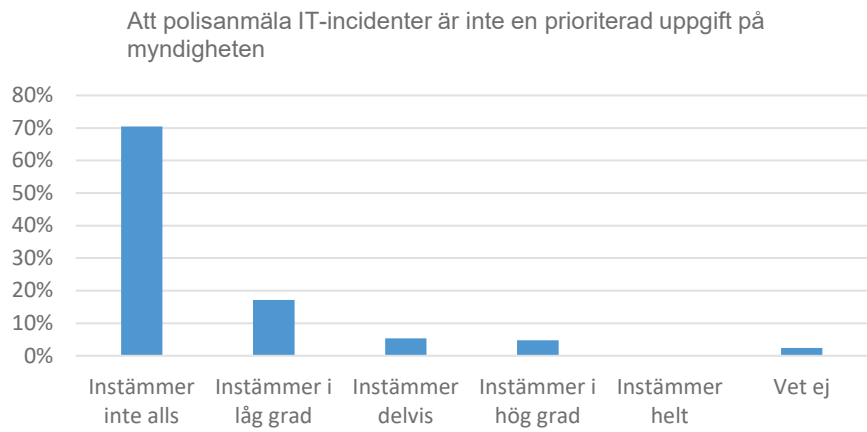
Den största andelen som instämmer *i låg grad* eller *inte alls* med påståendet återfinns i kategorin bevakningsansvariga myndigheter med 100 procent, följt av kategorin fler än 1000 anställda med 95 procent.



Figur 68: Fördelning av hur väl myndigheterna instämmer med påståendet om att ett medfört merarbete med polisanmälan av en IT-incident kan vara anledning till att polisanmälan uteblir, grupperat efter myndighetskategorier.

B.6.2 Ej prioriterad uppgift

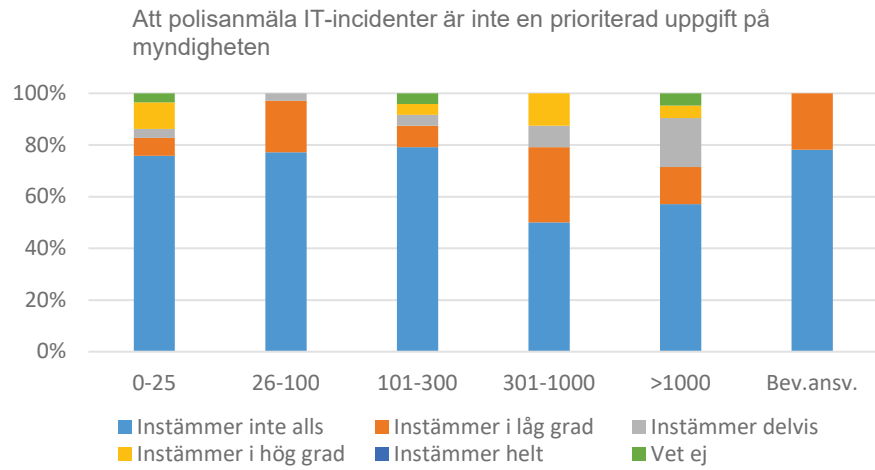
Bland samtliga myndigheter uppger 5 procent att de instämmer *i hög grad* eller *helt* med påståendet *att polisanmäla IT-incidenter är inte en prioriterad uppgift på myndigheten* skulle kunna vara en anledning till att polisanmälan av IT-incident inte sker. Motsvarande siffra för andelen som instämmer *i låg grad* eller *inte alls* är 88 procent.



Figur 69: Fördelning av hur väl myndigheterna instämmer med påståendet om att polisanmälan av IT-incidenter inte betraktas som en prioriterad uppgift vid myndigheten som anledning till att polisanmälan uteblir.

Den största andelen som instämmer *i hög grad* eller *helt* med att påståendet skulle kunna vara en anledning till att polisanmälan av IT-incident inte sker återfinns i kategorin 301-1000 anställda med 13 procent, följt av kategorin 0-25 anställda med 10 procent.

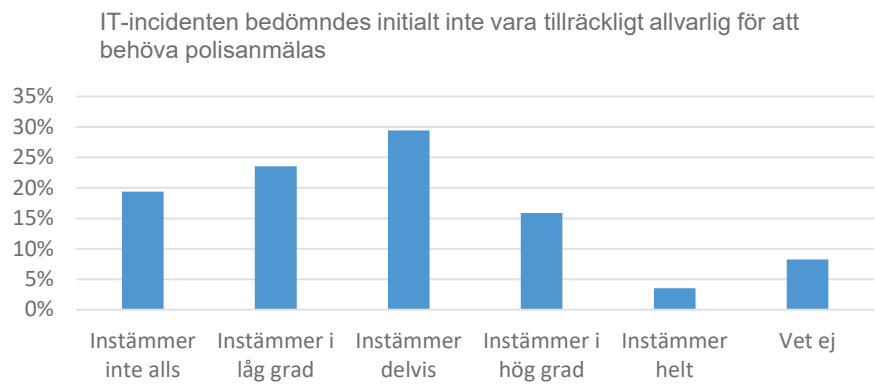
Den största andelen som instämmer *i låg grad* eller *inte alls* med att påståendet skulle kunna vara en anledning till att polisanmälan av IT-incident inte sker återfinns i kategorin bevakningsansvariga myndigheter med 100 procent, följt av kategorin 26-100 anställda med 97 procent.



Figur 70: Fördelning av hur väl myndigheterna instämmer med påståendet om att polisanmälan av IT-incidenter inte betraktas som en prioriterad uppgift vid myndigheten som anledning till att polisanmälan uteblir, grupperat efter myndighetskategorier.

B.6.3 Initialt inte tillräckligt allvarlig

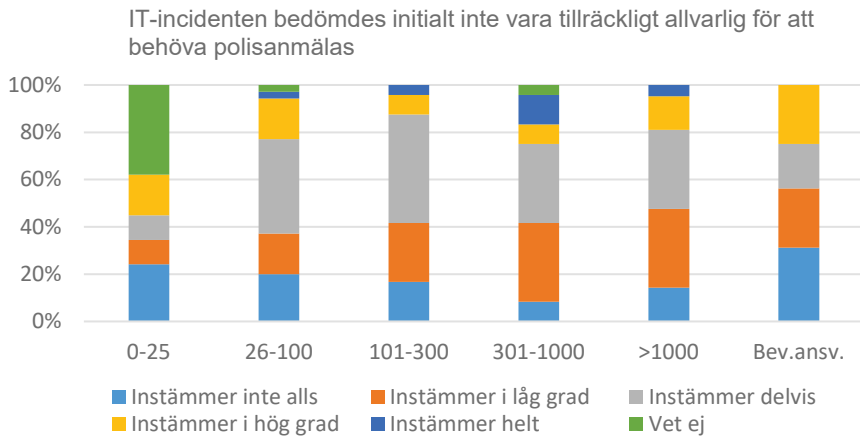
Bland samtliga myndigheter uppger 19 procent att de instämmer *i hög grad* eller *helt* med påståendet att *IT-incidenten bedöms initialt inte vara tillräckligt allvarlig för att behöva polisanmälas* skulle kunna vara en anledning till att polisanmälan av IT-incident inte sker. Motsvarande siffra för andelen som instämmer *i låg grad* eller *inte alls* är 43 procent.



Figur 71: Fördelning av hur väl myndigheterna instämmer med påståendet om att en initial bedömning att IT-incidenten inte är tillräckligt allvarlig för att polisanmälas kan vara anledning till att polisanmälan uteblir.

Den största andelen som instämmer *i hög grad* eller *helt* med att påståendet skulle kunna vara en anledning till att polisanmälan av IT-incident inte sker återfinns i kategorin bevakningsansvariga myndigheter med 25 procent, följt av kategorin 301-1000 anställda med 21 procent.

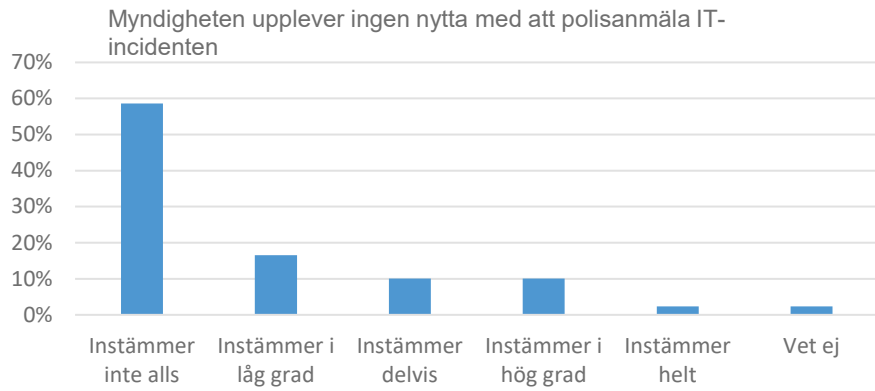
Den största andelen som instämmer *i låg grad* eller *inte alls* med att påståendet skulle kunna vara en anledning till att polisanmälan av IT-incident inte sker återfinns i kategorin bevakningsansvariga myndigheter med 56 procent, följt av kategorin fler än 1000 anställda med 48 procent.



Figur 72: Fördelning av hur väl myndigheterna instämmer med påståendet om att en initial bedömning att IT-incidenten inte är tillräckligt allvarlig för att polisanmälas kan vara anledning till att polisanmälan uteblir, grupperat efter myndighetskategorier.

B.6.4 Ingen upplevd nytta

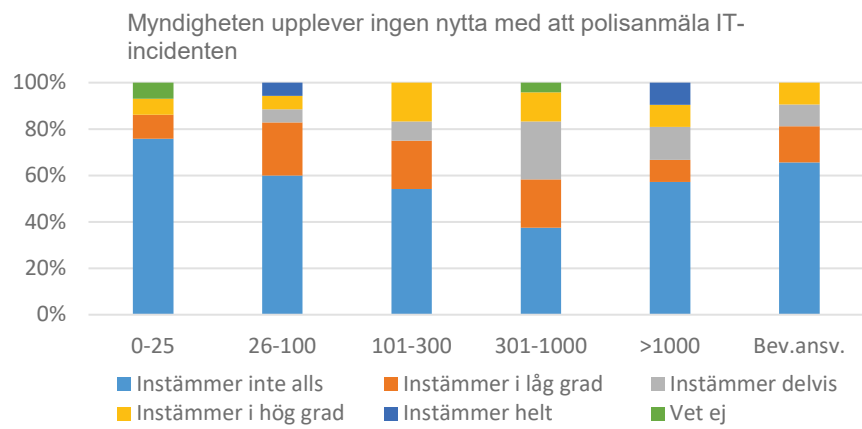
Bland samtliga myndigheter uppger 12 procent att de instämmer *i hög grad* eller *helt* med påståendet att *myndigheten upplever ingen nytta med att polisanmäla IT-incidenten* skulle kunna vara en anledning till att polisanmälan av IT-incident inte sker. Motsvarande siffra för andelen som instämmer *i låg grad* eller *inte alls* är 75 procent.



Figur 73: Fördelning av hur väl myndigheterna instämmer med påståendet om att icke upplevd nytta med polisanmälan kan vara anledning till att polisanmälan uteblir.

Den största andelen som instämmer *i hög grad* eller *helt* med att påståendet skulle kunna vara en anledning till att polisanmälan av IT-incident inte sker återfinns i kategorin fler än 1000 anställda med 19 procent, följt av kategorin 101-300 anställda med 17 procent.

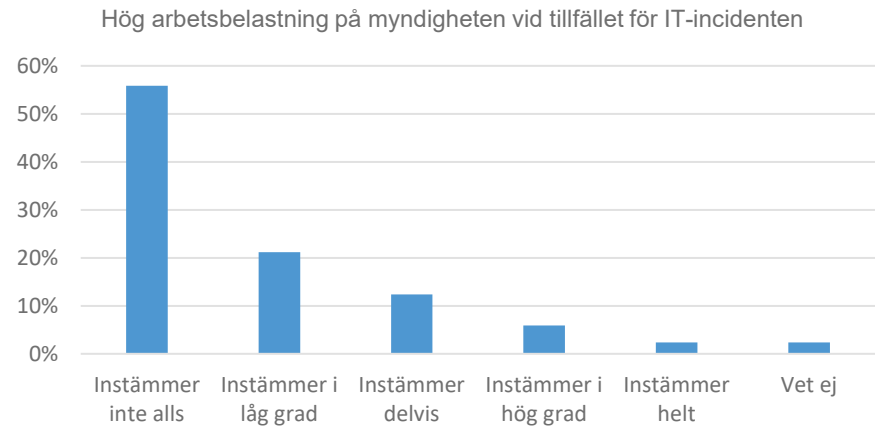
Den största andelen som instämmer *i låg grad* eller *inte alls* med att påståendet skulle kunna vara en anledning till att polisanmälan av IT-incident inte sker återfinns i kategorin 0-25 anställda med 86 procent, följt av kategorin 26-100 anställda med 83 procent.



Figur 74: Fördelning av hur väl myndigheterna instämmer med påståendet om att icke upplevd nytta med polisanmälan kan vara anledning till att polisanmälan uteblir, grupperat efter myndighetskategorier.

B.6.5 Hög arbetsbelastning på myndigheten

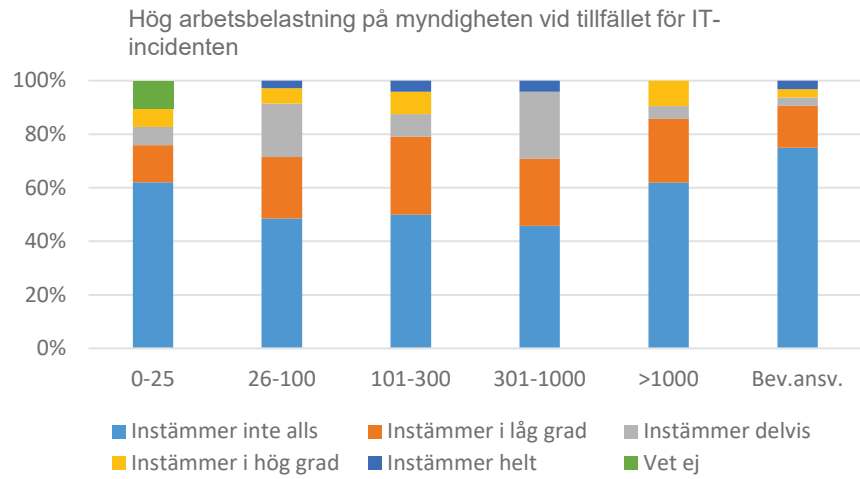
Bland samtliga myndigheter uppger 8 procent att de instämmer *i hög grad* eller *helt* med påståendet *hög arbetsbelastning på myndigheten vid tillfället för IT-incidenten* som möjlig anledning till att polisanmälan av IT-incident inte sker. Motsvarande siffra för andelen som instämmer *i låg grad* eller *inte alls* är 77 procent.



Figur 75: Fördelning av hur väl myndigheterna instämmer med påståendet om att hög arbetsbelastning på myndigheten vid tillfället för en IT-incident kan vara anledning till att polisanmälan uteblir.

Den största andelen som instämmer *i hög grad* eller *helt* med att påståendet skulle kunna vara en anledning till att polisanmälan av IT-incident inte sker återfinns i kategorin 101-300 anställda med 13 procent, följt av kategorin fler än 1000 anställda med 10 procent.

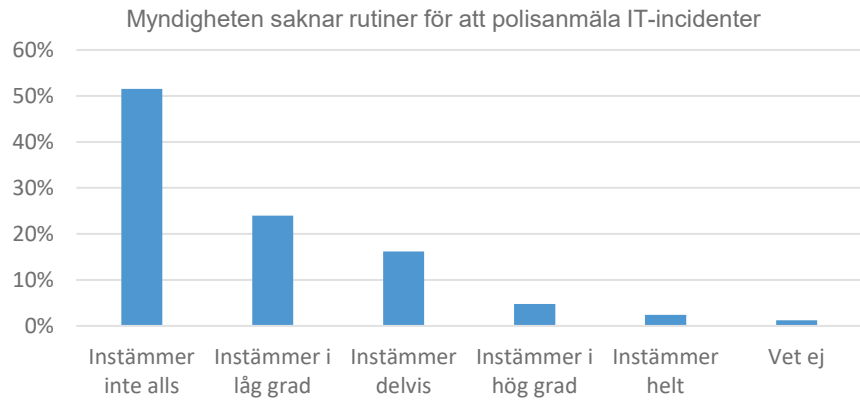
Den största andelen som instämmer *i låg grad* eller *inte alls* med att påståendet skulle kunna vara en anledning till att polisanmälan av IT-incident inte sker återfinns i kategorin bevakningsansvariga myndigheter med 91 procent, följt av kategorin fler än 1000 anställda med 86 procent.



Figur 76: Fördelning av hur väl myndigheterna instämmer med påståendet om att hög arbetsbelastning på myndigheten vid tillfället för en IT-incident kan vara anledning till att polisanmälan uteblir, grupperat efter myndighetskategorier.

B.6.6 Rutiner saknas

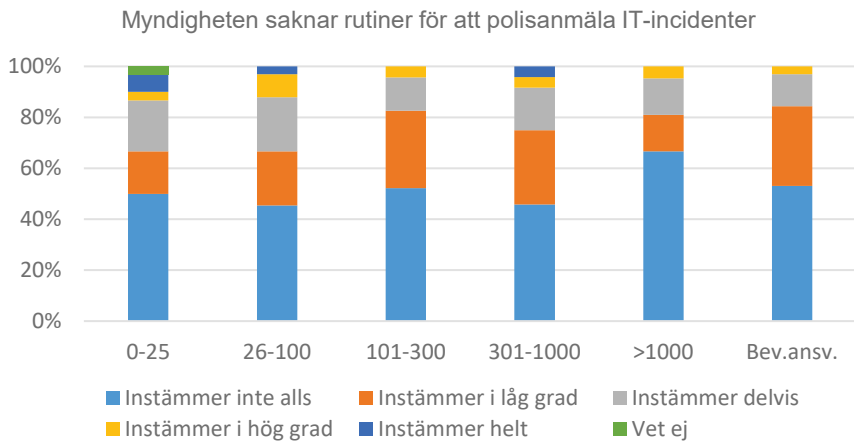
Bland samtliga myndigheter uppger 7 procent att de instämmer *i hög grad* eller *helt* med påståendet att *myndigheten saknar rutiner för att polisanmäla IT-incidenter* skulle kunna vara en anledning till att polisanmälan av IT-incident inte sker. Motsvarande siffra för andelen som instämmer *i låg grad* eller *inte alls* är 75 procent.



Figur 77: Fördelning av hur väl myndigheterna instämmer med påståendet om att en avsaknad av rutiner för polisanmälan av IT-incidenter kan vara anledning till att polisanmälan uteblir.

Den största andelen som instämmer *i hög grad* eller *helt* med att påståendet skulle kunna vara en anledning till att polisanmälan av IT-incident inte sker återfinns i kategorin 26-100 anställda med 12 procent, följt av kategorin 0-25 anställda med 10 procent.

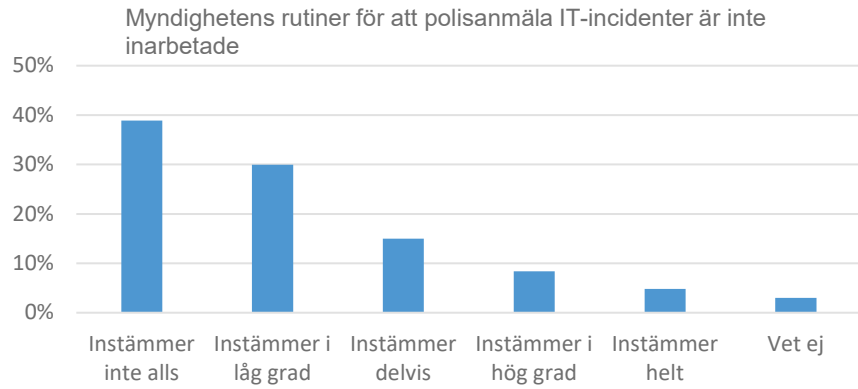
Den största andelen som instämmer *i låg grad* eller *inte alls* med att påståendet skulle kunna vara en anledning till att polisanmälan av IT-incident inte sker återfinns i kategorin bevakningsansvariga myndigheter med 84 procent, följt av kategorin fler än 1000 anställda med 81 procent.



Figur 78: Fördelning av hur väl myndigheterna instämmer med påståendet om att en avsaknad av rutiner för polisanmälan av IT-incidenter kan vara anledning till att polisanmälan uteblir, grupperat efter myndighetskategorier.

B.6.7 Ej inarbetade rutiner

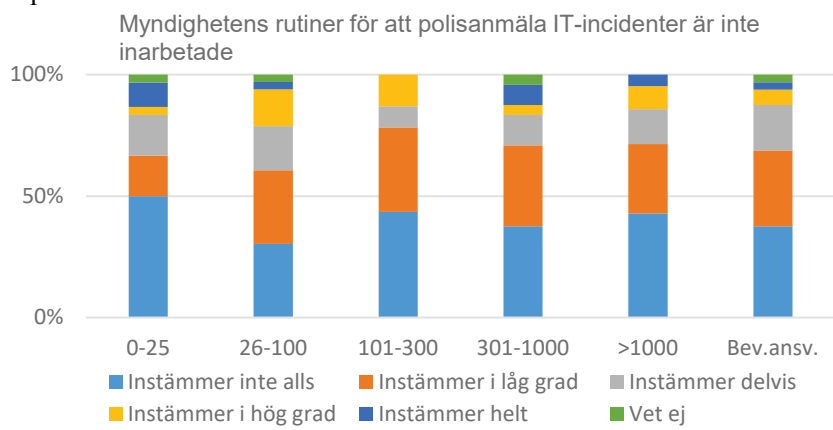
Bland samtliga myndigheter uppger 13 procent att de instämmer *i hög grad* eller *helt* med påståendet att *myndigheten saknar rutiner för att polisanmäla IT-incidenter* skulle kunna vara en anledning till att polisanmälan av IT-incident inte sker. Motsvarande siffra för andelen som instämmer *i låg grad* eller *inte alls* är 69 procent.



Figur 79: Fördelning av hur väl myndigheterna instämmer med påståendet om att icke inarbetade rutiner för polisanmälan av IT-incidenter kan vara anledning till att polisanmälan uteblir.

Den största andelen som instämmer *i hög grad* eller *helt* med att påståendet skulle kunna vara en anledning till att polisanmälan av IT-incident inte sker återfinns i kategorin 26-100 anställda med 18 procent, följt av kategorin fler än 1000 anställda med 14 procent.

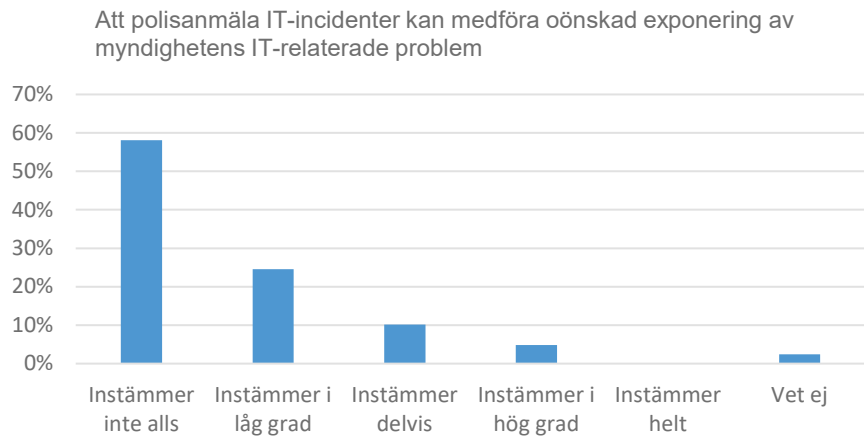
Den största andelen som instämmer *i låg grad* eller *inte alls* med att påståendet skulle kunna vara en anledning till att polisanmälan av IT-incident inte sker återfinns i kategorierna fler än 1000 anställda samt 301-1000 anställda, båda med 71 procent.



Figur 80: Fördelning av hur väl myndigheterna instämmer med påståendet om att icke inarbetade rutiner för polisanmälan av IT-incidenter kan vara anledning till att polisanmälan uteblir, grupperat efter myndighetskategorier.

B.6.8 Oönskad exponering

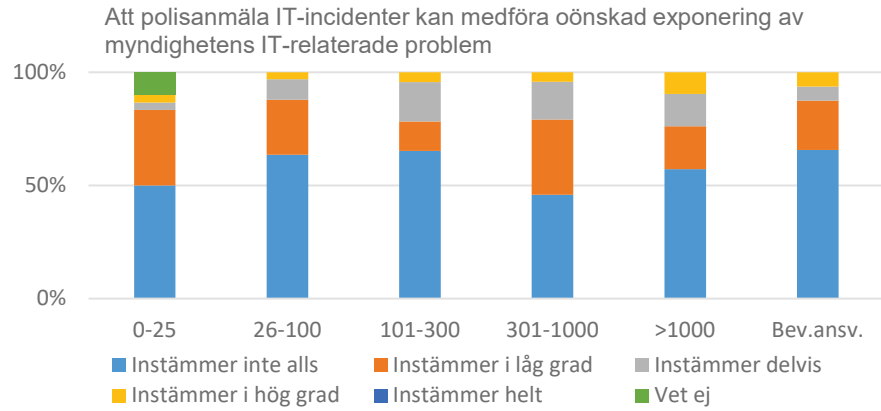
Bland samtliga myndigheter uppger 5 procent att de instämmer *i hög grad* eller *helt* med påståendet *att polisanmäla IT-incidenter kan medföra oönskad exponering av myndighetens IT-relaterade problem* skulle kunna vara en anledning till att polisanmälan av IT-incident inte sker. Motsvarande siffra för andelen som instämmer *i låg grad* eller *inte alls* är 83 procent.



Figur 81: Fördelning av hur väl myndigheterna instämmer med påståendet om att en medförd exponering av myndighetens IT-relaterade problem kan vara anledning till att polisanmälan av IT-incidenter uteblir.

Den största andelen som instämmer *i hög grad* eller *helt* med att påståendet skulle kunna vara en anledning till att polisanmälan av IT-incident inte sker återfinns i kategorin fler än 1000 anställda med 10 procent, följt av kategorin bevakningsansvariga myndigheter med 6 procent.

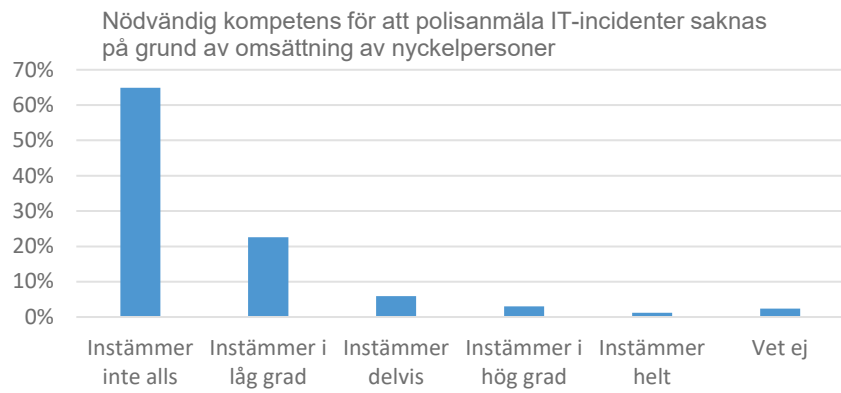
Den största andelen som instämmer *i låg grad* eller *inte alls* med påståendet återfinns i kategorierna bevakningsansvariga myndigheter samt 26-100 anställda, båda med 88 procent.



Figur 82: Fördelning av hur väl myndigheterna instämmer med påståendet om att en medförd exponering av myndighetens IT-relaterade problem kan vara anledning till att polisanmälan av IT-incidenter uteblir, grupperat efter myndighetskategorier.

B.6.9 Omsättning av nyckelpersoner

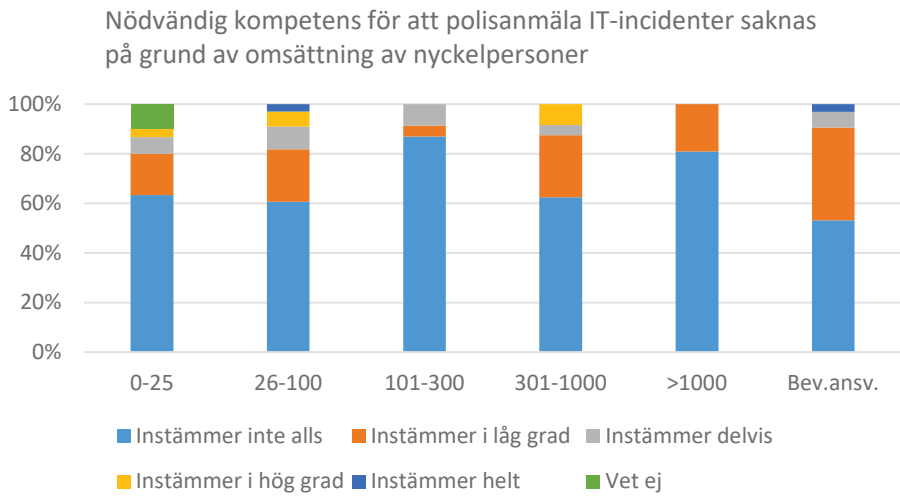
Bland samtliga myndigheter uppger 4 procent att de instämmer *i hög grad* eller *helt* med påståendet att *nödvändig kompetens för att polisanmäla IT-incidenter saknas på grund av omsättning av nyckelpersoner* skulle kunna vara en anledning till att polisanmälan av IT-incident inte sker. Motsvarande siffra för andelen som instämmer *i låg grad* eller *inte alls* är 88 procent.



Figur 83: Fördelning av hur väl myndigheterna instämmer med påståendet om att avsaknad av nödvändig kompetens på grund av personalomsättning av kan vara anledning till att polisanmälan av IT-incidenter uteblir.

Den största andelen som instämmer *i hög grad* eller *helt* med att påståendet skulle kunna vara en anledning till att polisanmälan av IT-incident inte sker återfinns i kategorin 26-100 anställda med 9 procent, följt av kategorin 301-1000 anställda med 8 procent.

Den största andelen som instämmer *i låg grad* eller *inte alls* med att påståendet skulle kunna vara en anledning till att polisanmälan av IT-incident inte sker återfinns i kategorin fler än 1000 anställda med 100 procent, följt av kategorierna bevakningsansvariga myndigheter samt 101-300 anställda, båda med 91 procent.



Figur 84: Fördelning av hur väl myndigheterna instämmer med påståendet om att avsaknad av nödvändig kompetens på grund av personalomsättning av kan vara anledning till att polisanmälan uteblir, grupperat efter myndighetskategorier.

Bilaga C. Myndigheternas förbättringsförslag

De enkätsvar som mottogs från de svarande myndigheterna resulterade i ytterligare ett resultat utöver de som återges i rapporten. Myndigheterna fick möjligheten att i fritext ge förslag på förändringar som de anser att MSB bör genomföra och som bedöms kunna leda till att myndigheternas rapportering av IT-incidenter ökar. I avsnitten som följer återges en sammanställning av de inkomna fritextsvaren. Sammanställningen återges inte nödvändigtvis utifrån hur många respondenter som har uttryckt det beskrivna, utan syftar snarare till att försöka återge de förslag som har inkommit från myndigheterna. I sammanställningen har det inte heller gjorts någon bedömning av de föreslagna förändringarnas rimlighet eller realiserbarhet.

C.1 Vad ska rapporteras?

Det upplevs kunna vara svårt att avgöra när en IT-incident är tillräckligt allvarlig för att den ska behöva rapporteras till MSB. Att myndigheterna själva har fått definiera var gränsen går för när en IT-incident blir tillräckligt allvarlig för att behöva rapporteras till MSB nämns som en möjlig orsak till att myndigheterna rapporterar i så olika utsträckning. En ytterligare möjlig orsak till skillnad i bedömning som nämns är att det varierar vilka mängder skyddsvärd information myndigheterna hanterar samt vilket ansvar för service de har mot allmänheten. En inträffad IT-incident kan därför bedömas ha olika dignitet beroende på aktuell myndighets verksamhet.

Ett önskemål som lyfts fram är tydliga exempel på hur MSB skulle bedöma allvarligheten för olika typer av händelser. MSB har i dagsläget en publikation[20] med exempel på hur olika typiska händelser skulle kunna bedömas, men fler och bättre exempel efterfrågas. Följande förslag ges på hur bedömningsstödet av IT-incidenters allvarlighet skulle kunna förbättras.

- Använd praktiska exempel från verkligheten där tveksamheter om bedömningen av allvarlighet har uppstått, gärna från olika typer av verksamheter för att förbättra stödet för myndigheter i att kalibrera vilka IT-incidenter som ska rapporteras.

[20] Exempel på IT-incidenter – Typexempel inklusive bedömning, https://www.msb.se/siteassets/dokument/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/it-incidentrapportering/exempel-pa-it-incidenter-april-2016.pdf

- Ha med exemplen på typiska incidenter som MSB inte anser ska rapporteras.
- Tydliggör att rapporteringsskyldigheten även omfattar allvarliga avvikelser som skulle kunnat ha resulterat i allvarliga störningar.
- Återkoppla till myndigheterna på insända IT-incidentrapporter så att myndigheterna vet om det är rätt typ av incidenter de rapporterar.
- Inför krav på att varje myndighet har en incidenthandläggare som ingår i ett MSB-forum där regelbundna möten och utbildningar används som ett sätt att harmonisera bedömningskriterier och använda metoder i syfte att nå önskad inrapporteringskvalitet.

C.2 Rapporteringsförfarandet

Dagens krav på att en IT-incident ska rapporteras till MSB inom 24 timmar från det att den bedömts som allvarlig är för snävt. I en situation där en incident har inträffat och det är skarpt läge så har inte rapporteringen högsta prioritering. Det kan även vara så att rapporteringsansvarig på myndigheten arbetar normal kontorstid och att det inte finns möjlighet att ha beredskap dygnet runt för rapportering. Detta beskrivs dock inte som anledningar att inte rapportera, utan kan snarare vara förklaringar till varför rapporteringar inkommer sent. Följande förslag ges på hur problemet med för snäv rapporteringstid skulle kunna hanteras.

- Ändra tidsgränsen för rapportering till 72 timmar, vilket är samma som Datainspektionen har.
- Möjliggör rapportering av ofullständiga rapporteringsunderlag som kan kompletteras vartefter mer fakta om IT-incidenten finns tillgänglig.
- Ändra så att tidsgränsen på 24 timmar enbart gäller incidenter som kan ha bäring på andra aktörer och ha istället en tidsgräns på 72 timmar för incidenter som i huvudsak blir statistik på aggregerad nivå.

Dagens rapporteringsförfarande med en blankett som ska fyllas i och mailas till MSB anses omständligt. Istället efterfrågas ett förenklat förfarande där rapporteringen sker via ett webbaserat gränssnitt. Med ett webbaserat gränssnitt skulle det vara möjligt att ha smartare formulär som anpassas utifrån vad som rapporteras. I dagsläget kan krävas att rapporteringen hanteras i flera olika system. Det föreslås därför att det webbaserade systemet tillgängliggör ett API[21]

[21] Applikationsprogrammeringsgränssnitt (eng. Application Programming Interface), vilket är en specifikation av hur viss programvara kan användas av annan programvara.

som myndigheterna kan använda för enklare samordning mellan rapportering till olika IT-system.

För att hantera att information om en inträffad IT-incident kan omfattas av sekretess sker rapportering i dagsläget med hjälp av Kurir, vilket lyfts fram som en förlegad och icke-flexibel lösning. Det nämns även att det kan vara få personer inom organisationen som har tillgång till Kurir, vilket ökar personberoendet när rapportering ska genomföras. Som ett alternativ till rapportering med Kurir föreslås att ovan föreslagna webbaserade gränssnitt exempelvis tillhandahålls via Swedish Government Secure Intranet (SGSI). På så sätt bedöms fler av inblandad personal, exempelvis IT-tekniker, kunna genomföra rapporteringen till MSB, vilket skulle kunna minska den administrativa bördan och leda till snabbare inrapportering till MSB.

Avseende sekretess efterfrågas att inkomna IT-incidentrapporter inte blir offentliga då det anses kunna avskräcka myndigheter från att rapportera incidenter om det finns en risk att information om myndighetens brister och svagheter blir publika. Förslagsvis ges myndigheten större möjligheter att sekretessklassificera IT-incidentrapporteringarna och därmed även hur rapporten ska hanteras av MSB.

I syfte att förbättra rapporteringsförfarandet ges även följande förslag:

- Tillhandahåll en förbättrad support på MSB som kan stödja i grundläggande bedömning av huruvida rapportering ska ske.
- Inför ett förenklat rapporteringsförfarande för händelser som är av mindre allvarlig art alternativt för händelser som redan är kända genom media och som redan har spritts till många organisationer.
- Koordinera rapporteringen av IT-incidenter till MSB med rapportering till Polismyndigheten och Datainspektionen, vilket i sin enklaste form skulle kunna ske genom korsreferenser till respektive rapporteringssystem.
- Skapa en lathund för rapporteringsförfarandet som myndigheterna kan använda när en IT-incident har inträffat då det kan upplevas som en stressig situation när rapporteringsansvariga har mycket att göra.

C.3 Återkoppling

Dagens återkoppling från MSB upplevs primärt utgöras av den rapport som CERT-SE varje månad skickar ut till de rapporteringsskyldiga myndigheterna. Att en månadsrapport skickas ut lyfts fram som positivt, men primärt från bevakningsansvariga myndigheter efterfrågas högre detaljeringsgrad för att rapporten ska kunna fylla funktionen att informera myndigheter om hur risker

kan hanteras. Månadsrapporten föreslås återrapportera mer avseende hot och händelser som MSB har fått information om via myndigheternas IT-incidentrapportering. För att myndigheterna ska kunna lära sig av varandras IT-incidenter föreslås att månadsrapporterna blir mer fylliga och inkluderar information om vad som har orsakat incidenter, vilka sårbarheter som möjliggjorde incidenten samt vilka skydd eller åtgärder som hade kunnat förebygga incidenten. Med sådan information har myndigheterna ett underlag de kan agera på som bidrar till förbättrat IT-arbete eller förmåga att upptäcka och förhindra IT-incidenter i sin IT-miljö. Om rapporterna avidentifieras för mycket så tillför de i princip inte något.

Det påpekas att dagens månadsrapporter hamnar hos myndighetens registratur, vilket gör det omständligt att få tillgång till dem. Alternativ lösning som föreslås är att CERT-SE tillhandahåller en egen app där berörda personer på myndigheterna med hjälp av Bank ID kan ta del av information.

När myndigheter rapporterar in IT-incidenter till MSB upplevs det som att de inte får någon återkoppling på det som har rapporterats in. Som en följd kan det upplevas som att rapporteringen huvudsakligen är av statistisk betydelse, vilket inte bör vara fallet. Om MSB skulle ge direkt återkoppling till berörd myndighet om den bedömning de gör av varje rapporterad IT-incident skulle den upplevda nyttan öka. Om återkopplingen även skulle kombineras med förslag på åtgärder, alternativt uppföljning av att lämpliga åtgärder har vidtagits, skulle den upplevda nyttan öka ytterligare. Genom återkoppling på rapporterade IT-incidenter skulle de rapporteringsskyldiga myndigheterna kunna arbeta tillsammans med MSB på ett sätt som inte är möjligt utan återkoppling. Förbättrad återkoppling på rapporterade IT-incidenter anses även kunna gynna förtroendet för MSB:s IT-säkerhetsarbete och understryka nyttan med själva rapporteringen.

Som ett första steg i att förbättra återkopplingen föreslås att det för alla rapporterade IT-incidenter skickas en bekräftelse till berörd myndighet att rapporteringen har mottagits. Bekräftelsen föreslås innehålla ett löpnummer eller diarienummer som framöver kan användas som referens.

C.4 Utbildning

Myndigheternas tillgängliga IT-resurser varierar, exempelvis utifrån myndighetens storlek. Det lyfts att information om IT-incidentrapporteringen tydligare bör spridas till nya myndigheter som inte har hunnit skapa rutiner för IT-incidentrapportering. Det föreslås även att MSB tillhandahåller lättillgängliga webbutbildningar som ger en introduktion till IT-säkerhetsarbete och IT-incidentrapportering. Det kan även vara så att det krävs en tydligare uppsökande verksamhet hos MSB för att erbjuda utbildningar till rapporteringsskyldiga

myndigheter. Regelbundet återkommande tillfällen för utbildning och övning i IT-incidentrapportering i MSB-regi föreslås.

MSB föreslås i större utsträckning bjuda in till informationsdagar eller seminarier för att ge mer allmän uppdatering och utbildning till myndigheterna.

ISSN 1650-1942

www.foi.se