NORDISKT SAMARBETE OM INFORMATIONSSÄKERHET I KOMMUNER, REGIONER OCH LANDSTING

PROMEMORIA OM INFORMATIONSSÄKERHET OCH DIGITALISERING

SVENSKA LANDSTING OCH REGIONER 2015

2008–2015

Promemorian är utarbetad för:

Sveriges Kommuner och Landsting

Augusti 2015

INLEDNING

Digitalisering i form av självbetjäningslösningar för medborgare och verksamheter, nya möjligheter till virtuell kommunikation med omvärlden, mobila och flexibla arbetsplatser och användningen av sociala medier i yrkesmässiga och privata sammanhang betyder att databehandlingen flyttas från stora system och manuella processer till nya digitala plattformar.

Riskbilden för informationsanvändningen framstår på flera områden som mer omfattande och komplex än förut.

- Datas pålitlighet och trovärdighet kontrolleras oftare genom system än av människor.
- Data- och systemtillgänglighet är i fokus när åtkomsten till information sker genom system.
- Data kan vara belägna på många olika IT-plattformar i landstinget som oftast endast delvis är under landstingets kontroll.

Informationssäkerhet är ett område som får stor uppmärksamhet bland allmänheten:

- En kommande EU-förordning skärper kraven på behandling av känsliga personuppgifter och fastställer bland annat krav på ansvarsskyldighet.
- En rad händelser har visat hur sårbara IT-system är för kriminella handlingar samt interna fel och internt missbruk.

God praxis för informationssäkerhet beskrivs i standarden ISO 27001 som tar utgångspunkt i en närmare förbindelse mellan förvaltningsorganisationen och den nödvändiga nivån av informationssäkerhet, men utan att föreskriva konkreta minimiinsatser. SKL rekommenderar att landstingen använder ISO-standarden i syfte att få en gemensam hög säkerhetsstandard inom den offentliga sektorn. Detta innebär en rad förväntningar på organisationens kompetens och förmåga att arbeta med informationssäkerhet gällande

- den övre ledningens ansvar för mål och uppföljning av organisationens informationssäkerhet
- förvaltningsorganisationens ansvar för att organisera en säker IT-användning.

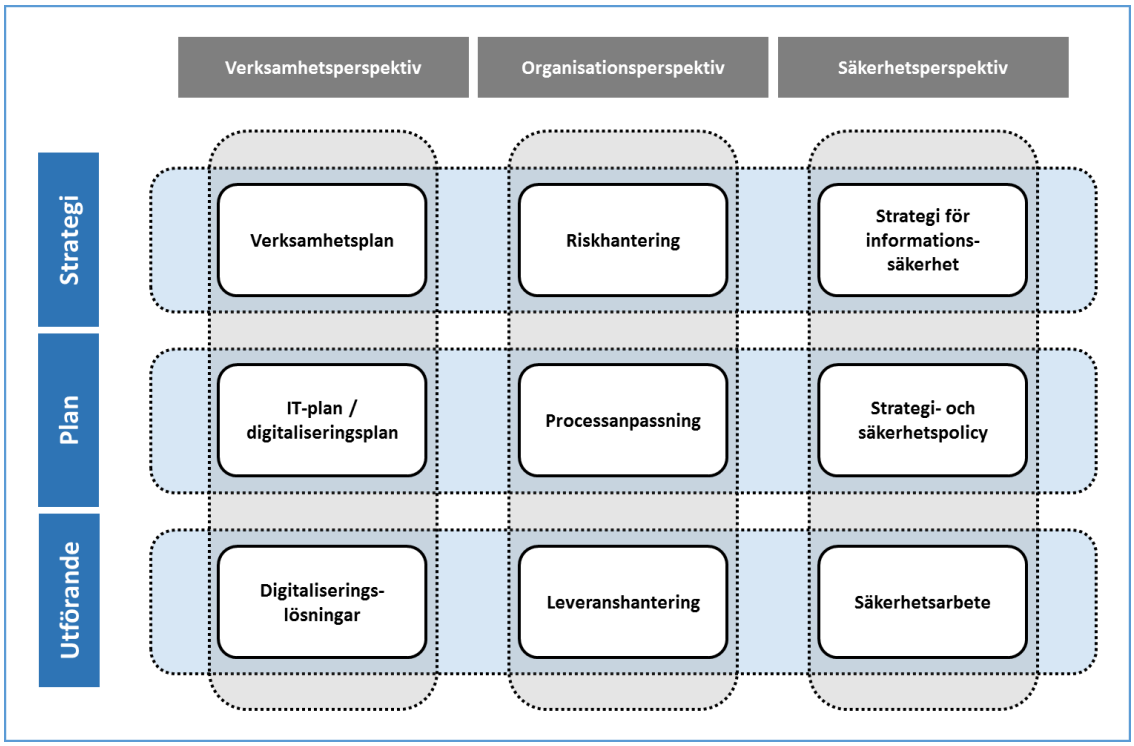
Promemorian visar hur långt svenska landsting har kommit inom dessa områden och hur ramverket för informationssäkert har organiserats.

Undersökningens frågetema är utformat så att det avspeglar organisationens samlade fokus på informationssäkerhet – från den övre ledningen till det konkreta arbetet. Dessutom har frågetemat fokus på landstingens användning av IT och de riskanalyser som utförs. Undersökningen har kvar frågor som knyter tillbaka till 2012 och tidigare, men strävar även efter att hitta trender i IT-användning och initiativ till säkrare alternativ.

Tidigast 2017 planeras en rad bestämmelser om skydd av personuppgifter att träda i kraft i enlighet med EU:s personuppgiftsförordning. Undersökningen innehåller en genomgång av tre av de fyra huvudområdena i förordningen. För dem som vill ha full täckning av det fjärde området finns det möjlighet att svara på extrafrågor.

Slutligen innehåller undersökningen en rad frågor om upplevda händelser och följderna av dessa.

Förhållandet mellan användning av system och information i verksamhetssyfte och landstingens bedömning av informationssäkerhet visas i modellen nedan.



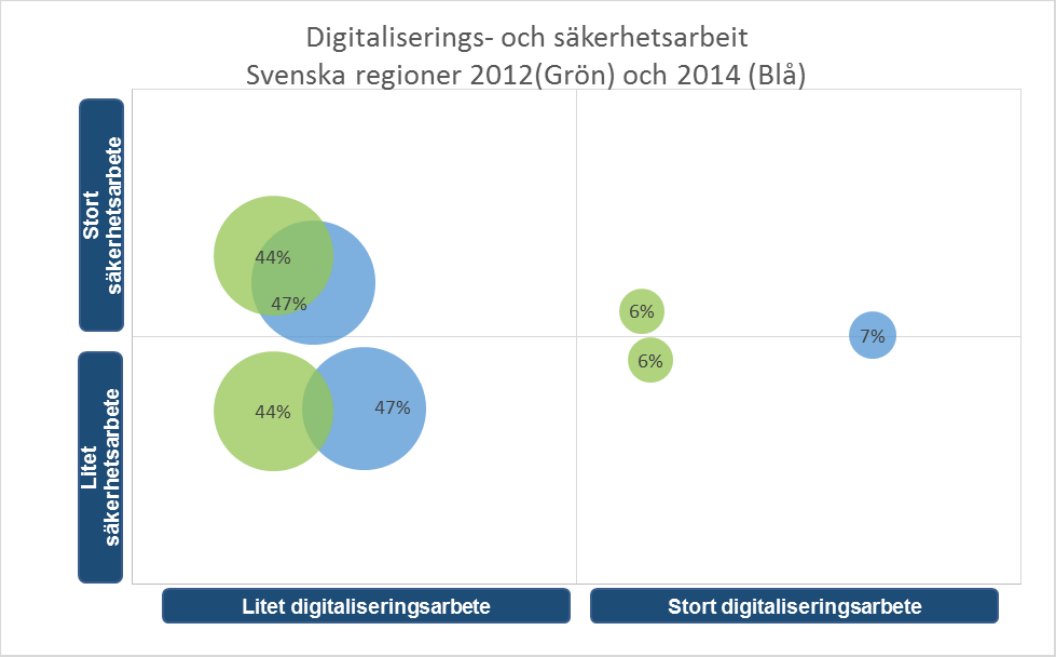
Promemorian är utformad med utgångspunkt i den nordiska undersökningen om informationssäkerhet i kommuner och regioner. 16 av de 21 landstingen har svarat på undersökningen.

Kommuner och landsting har tillgång till självskattningsverktyget NordSec som användes för undersökningen och de organisationer som inte deltog kan även under 2016 svara på frågorna, se sin egen status och jämföra sig med övriga svenska och nordiska organisationer.

INFORMATIONSSÄKERHET OCH DIGITALISERING

Det samlade arbetet

NordSecs undersökning ger möjligheten att se den yrkesmässiga användningen av IT för patientadministration och -behandling i förhållande till säkerhetsinitiativen.

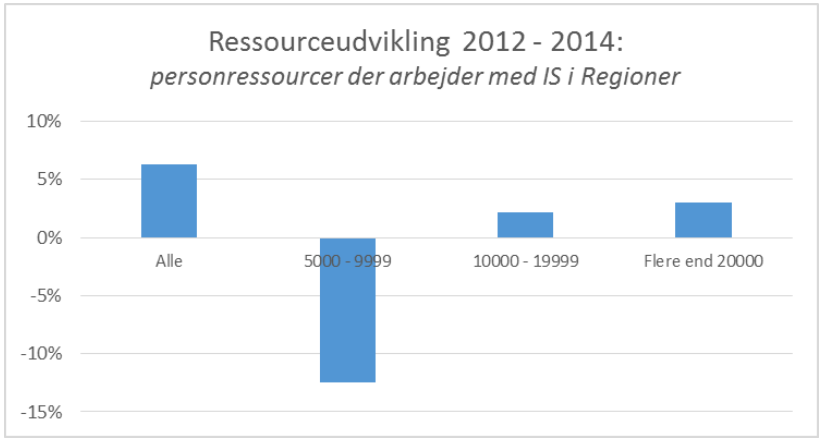


De senaste åren har det funnits en stor fokus på att använda digitala lösningar för dialogen med patienter (kallelser m.m.) och i behandlingssammanhang. Diagrammet visar en tydlig förflyttning sedan 2012 mot en större grad av digitalisering. Under samma period kan man se att uppmärksamheten på informationssäkerhet har minskat i en större grupp av landstingen. 40 % ligger på en fortsatt låg nivå av informationssäkerhet.

Resursinsatser

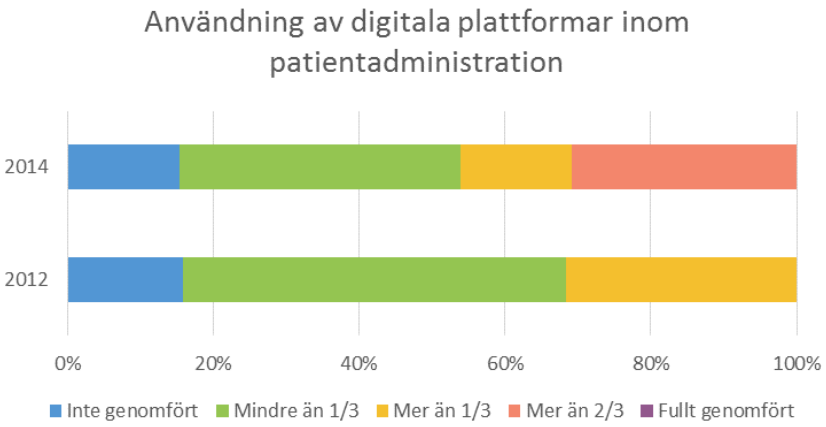
Från 2012 till 2014 ses en mindre ökning av antalet personresurser som arbetar med informationssäkerhet i landstingen. Var tredje län har under 10 000 anställda. Denna grupp har minskat sedan 2012.

I snitt är det 3,2 personer i varje län som arbetar med informationssäkerhet.



Digitalt arbete

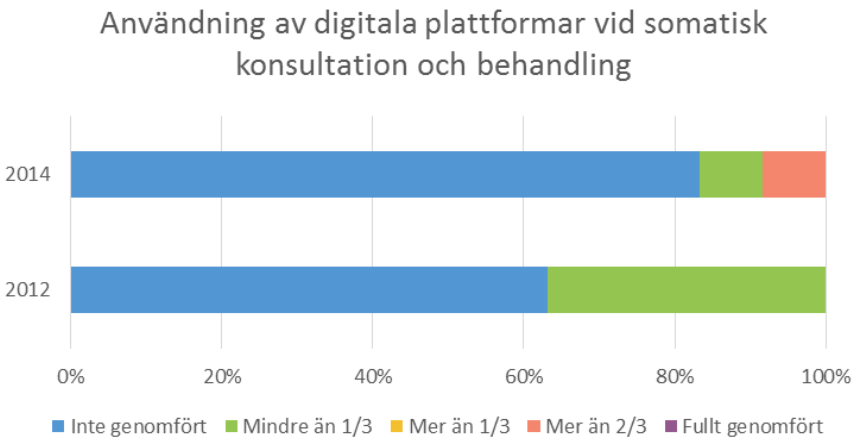
Det digitala arbetet illustreras i undersökningen av tre områden – dialogen med patienter och remitterande läkare, användning av IT i patientens behandling inom det somatiska området och motsvarande inom det psykiatriska området.



Patientadministration omfattar tre enskilda områden där man kan se en förändring 2012–2014. Det kan på alla tre områden ses en markant utveckling sedan 2014:

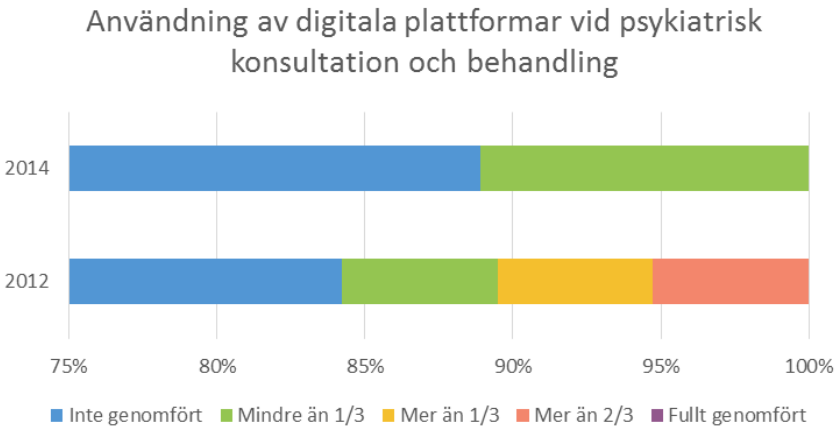
- Alla landsting arbetar med digital kommunikation tillsammans med andra myndigheter när det gäller patientuppgifter vid utskrivning.
- Vartannat landsting arbetar med patienters tillgång till journaluppgifter.
- Var fjärde landsting har möjligheten att kalla patienter via SMS eller e-post.

Frågorna om IT-användning inom det somatiska området omfattade fyra enskilda områden: konsultation via videoförbindelse, övervakning av patientparametrar, stöd av terapeutisk behandling (behandling av sår osv.) och annan terapeutisk behandling i hemmet:



12 av de 16 deltagande landstingen svarade på frågorna och nedgången i användning var jämnt fördelad över de fyra områdena.

Frågorna om IT-användning inom det psykiatriska området omfattade två områden: konsultation via videoförbindelse och behandling via videoförbindelse.

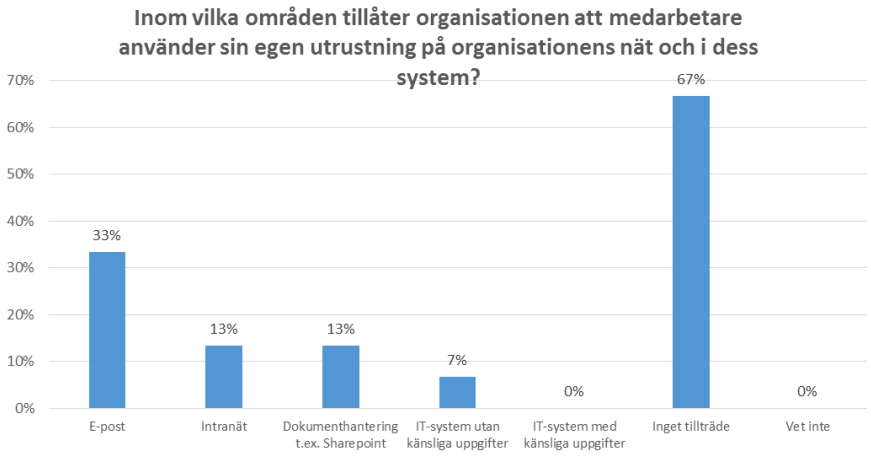


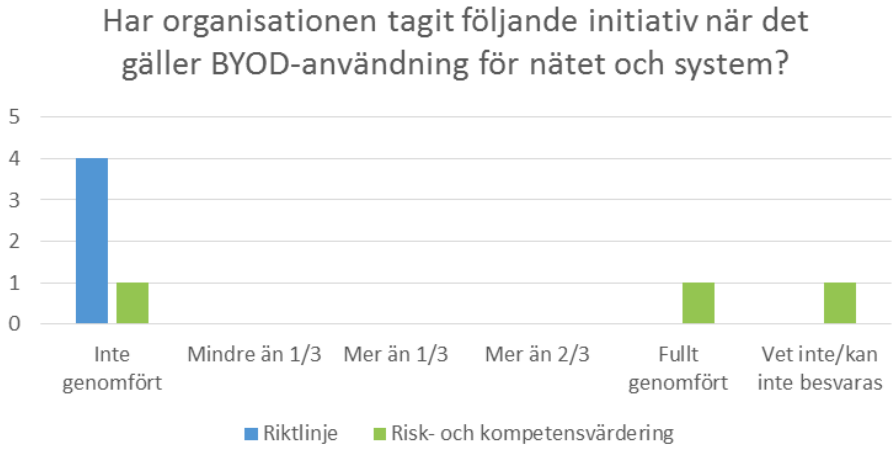
9 av de 16 deltagande landstingen svarade på frågorna.

Ny teknik

Under de senaste åren har det skett en betydlig spridning av den utrustning som används tillsammans med informationssystemen (mobila arbetsplatser, telefoner osv.). Denna trend förstärks av att medarbetare i allt större omfattning efterfrågar möjligheten att använda sin egen utrustning på organisationernas nät – både privat och för uppgifter. I

undersökningen 2012 svarade fyra av landstingen att de planerade att tillåta det och två att de tillät det i begränsad omfattning.



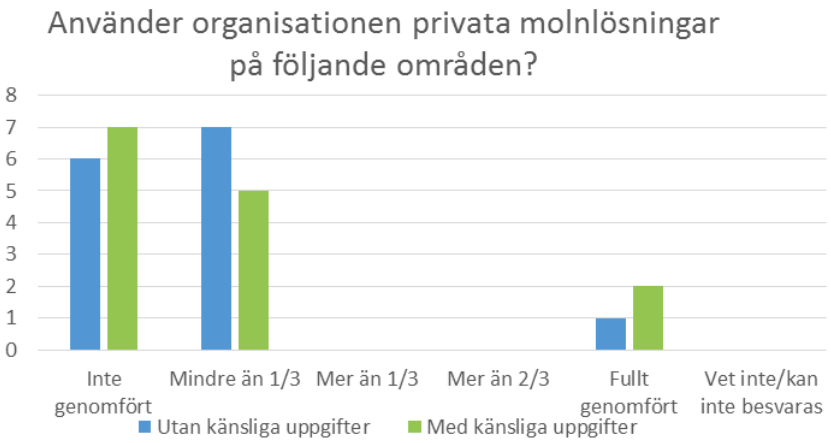


I 2014 tillåter var tredje landsting att medarbetarna använder egen utrustning för åtkomst till landstingens e-postsystem och i begränsad omfattning till andra områden. Inget av landstingen tillåter åtkomst till system med känsliga uppgifter.

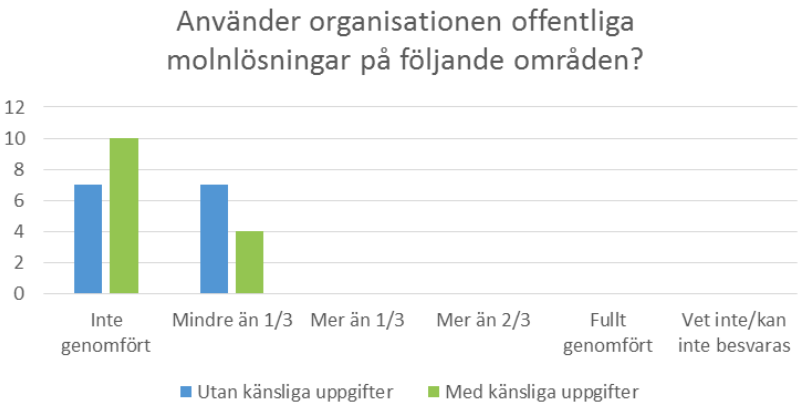
Ett av de landsting som tillåter att medarbetare använder egen utrustning till landstingens nät och system har genomfört en risk- och konsekvensanalys och inget av landstingen har riktlinjer för området.

Användning av molntjänster

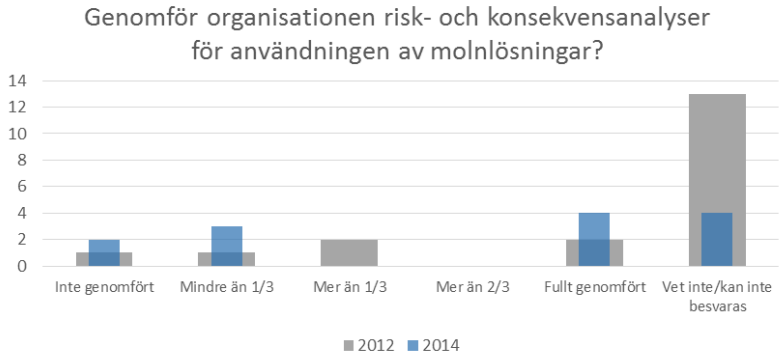
Användningen av molntjänster på områden som innehåller personupplysningar har diskuterats länge i Sverige. Det är få landsting som använder dedicerade (privata) molntjänster och användningen är mycket begränsad om personuppgifter är involverade.



När det gäller användningen av offentliga molnlösningar framgår att landstingen i en begränsad omfattning använder dem för både känsliga och icke-känsliga uppgifter.



Det finns ett antal rekommendationer som handlar om säkerhetshantering i samband med användningen av molnlösningar. Det är avgörande att organisationer tar ställning till de risker de som är kopplade till molnbaserade tjänster.

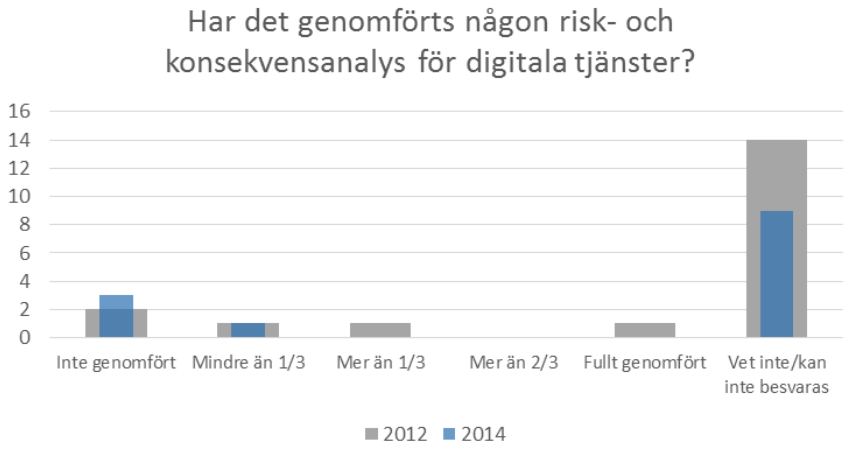


Utvecklingen sedan 2012 visar en ökande uppmärksamhet på området och att användningen av molnlösningar oftare ses utifrån en riskanalys.

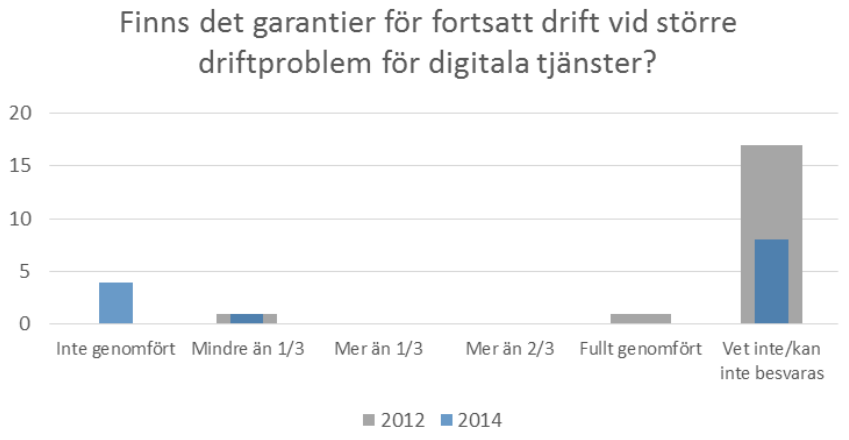
Riskhantering för digitala lösningar

I samband med införandet av digitala lösningar i behandlingen av patienter och i den patientriktade dialogen ändras riskbilden på flera områden – hot mot både tjänsternas tillgänglighet och informationens trovärdighet samt konsekvenserna av ett brott mot efterlevnad skiftar karaktär.

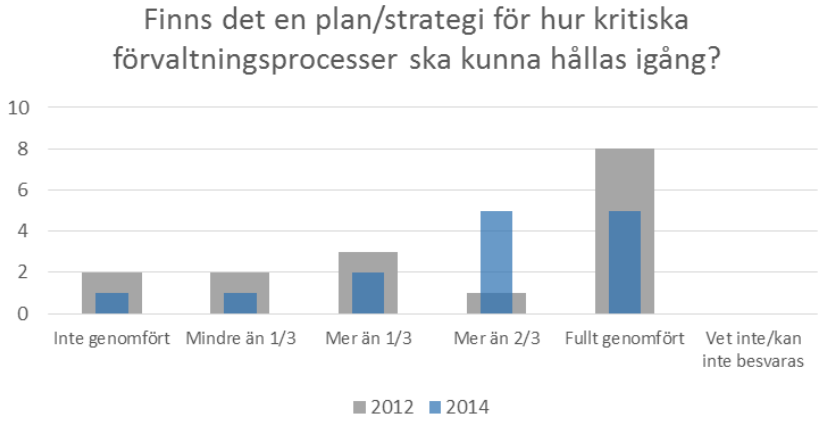
De tillfrågade i landstingen är tydligen inte inblandad i de processer där risk- och konsekvensanalyser genomförs för digitala lösningar. En större andel har ingen vetskap om detta och de övriga bedömer att de inte har genomförts.



I och med omläggningen till digitala tjänster ligger kraven inte uteslutande på medarbetares och systems tillgänglighet utan även på medborgares och verksamheters tillgång till digitala tjänster.
En del av de tillfrågade anser att det inte har vidtagits några särskilda initiativ för fortsatt drift, medan vissa inte har kunskap om området.



Landstingen är i ökande omfattning uppmärksamma på att kritiska processer måste kunna hållas igång om det uppstår problem med tillgång till IT eller andra kritiska resurser. Mer än två tredjedelar av landstingen har en Business Continuity Plan, dvs. en plan för hur tjänster ska kunna utföras om kritiska resurser inte finns tillgängliga.

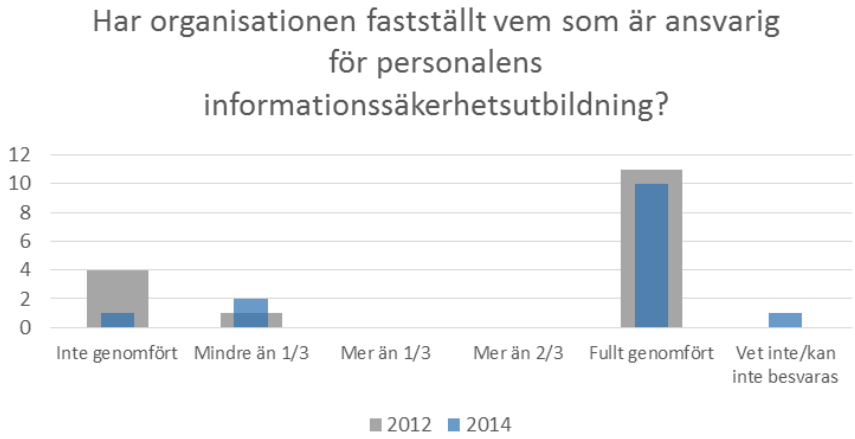


En fungerade Business Continuity Plan förutsätter lokala handlingsplaner för enskilda förvaltningsområden: sju av tio landsting har en sådan helt eller delvis på plats i jämförelse med fem av tio 2012. Var tredje landsting har en plan för regelbunden utbildning och testning av sin beredskap.

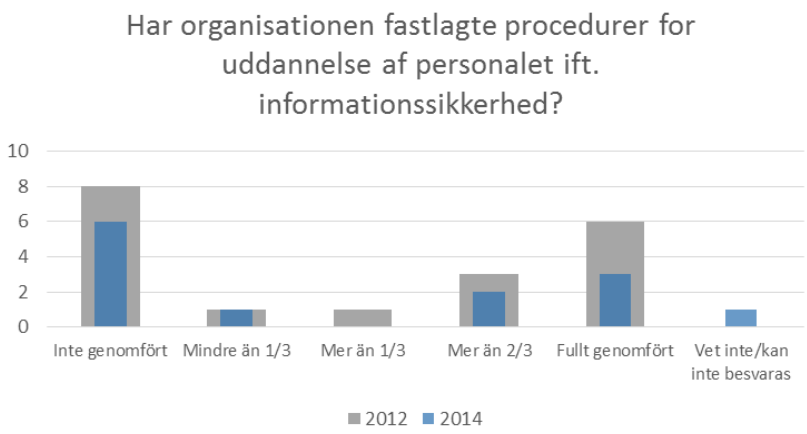
Kompetenskrav för organisationen

I och med användningen av digitala tjänster och digitala plattformar – e-post, digital dialog, m.m. – möts medarbetare av andra och annorlunda utmaningar än förr.

Det framgår att 3 av 4 landsting har slagit fast ett formellt ansvar inom organisationen för att medarbetare ska ha tillräcklig och relevant kompetens för säker användning.



Var tredje landsting har slagit fast ett ramverk för genomförandet av personalutbildning – samma antal som 2012. Hälften av landstingen arbetar inte med det området.

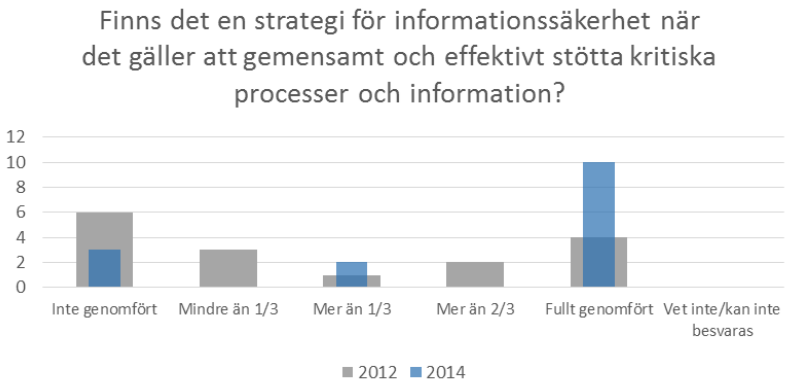


2012 hade två av landstingen avsatt medel till arbete för att utbilda medarbetarna i säker användning av information och informationsteknik – samma antal gäller 2014.

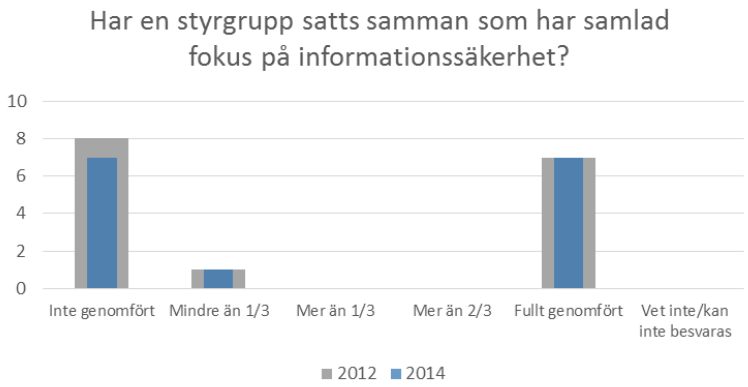
2012 hade ett av landstingen ett förfarande för att undersöka om medarbetarna hade tillräcklig kompetens för att säkert använda system och information. Detsamma gäller 2014, då ett av landstingen arbetar med sådana analyser. Landstinget rapporterar mätningsresultaten till den övre ledningen.

Informationssäkerhet inom organisationen

Införandet av digitala tjänster och användningen av digitala plattformar genomförs i nära samarbete med landstingens förvaltningsområden. Två tredjedelar av landstingen arbetar med en strategi för hur hänsyn kan tas till informationssäkerhet under införandet av ny teknik. Siffrorna har ökat i jämförelse med 2012.

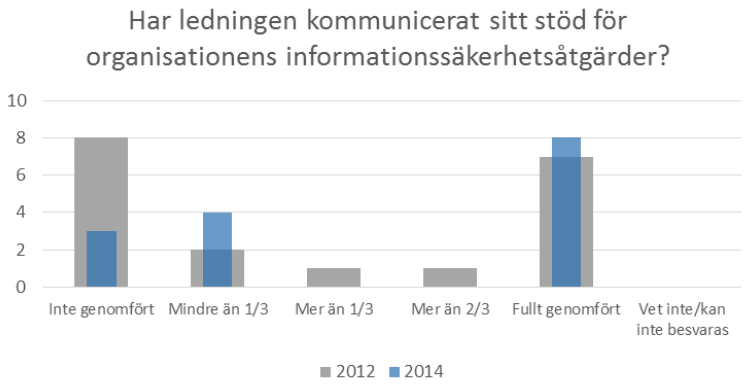


Förankringen av informationssäkerhetsarbetet inom organisationen omfattar i hälften av landstingen etableringen av styrgrupper som har samlad fokus på området.

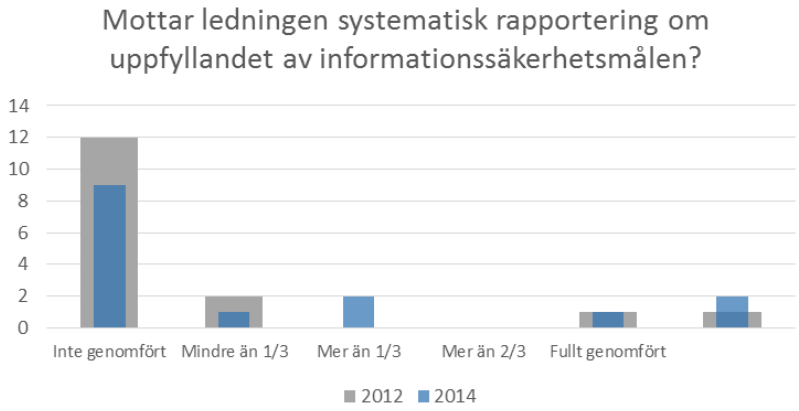


Informationssäkerhet som ledningsområde

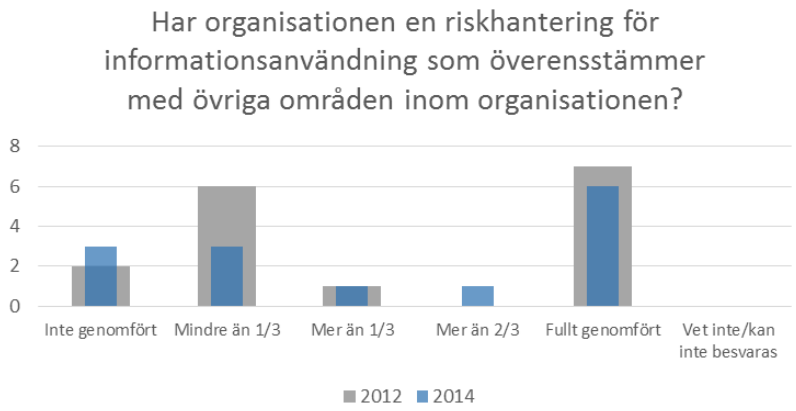
Ledningens synliga stöd för organisationens informationssäkerhetsarbete framhävs ofta som en avgörande faktor för god praxis. Sådant stöd finns i hälften av landstingen och är samlat sett en ökning.



Siffrorna ser annorlunda ut för om ledningens stöd för informationssäkerhetsarbete följs upp av regelbunden och systematisk statusrapportering till ledningen. Under 10 % av landstingen arbetar med detta.



Riskhanteringsunderlag är ett av de områden där ledningen kan ha inflytande över säkerhetsarbetet. Detta inflytande kan utövas genom att säkerställa att de metoder som används är välkända och liknar organisationens övriga riskhantering samt att de risker som identifieras övervägs enhetligt.



Nästan hälften av landstingen har genomfört en riskanalys för IT-användning vilken överensstämmer med organisationens övriga riskhantering.

Var fjärde landsting har utarbetat kriterier för vad som räknas som acceptabla risker.

För de landsting som inte har samlad fokus på risker kan riskhanteringen av IT-användning bli avskuren från resten av riskhanteringen i organisationen.