



LUNDS UNIVERSITET

Ekonomihögskolan

Institutionen för informatik

Informationssäkerhetsutmaningar i samband med digitalisering av HR-processer

Kandidatuppsats 15 hp, kurs SYSK16 i Informatik

Författare: Louise Wetterlundh

Handledare: Christina Keller

Rättande lärare: Markus Lahtinen
Magnus Wärja

Informationssäkerhetsutmaningar i samband med digitalisering av HR-processer

ENGELSK TITEL: Information security challenges in relation to digitalization of HR-processes

FÖRFATTARE: Louise Wetterlundh

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Osama Mansour, PhD

FRAMLAGD: maj, 2022

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 73

NYCKELORD: HR-digitalisering, digitalisering, säkerhetsutmaningar, informationssäkerhet

SAMMANFATTNING (MAX. 200 ORD): Digital-HR och digitala HR-verktyg har utvecklats i syfte att generera en värdefull informationsdatabas över de mänskliga resurserna i en organisation. Genom att digitalisera mer inom HR frigörs ytterligare tid till organisationsutveckling och människorna i organisationen. En effekt av digitaliseringen är ökat behov av informationssäkerhet i organisationerna. Digitala lösningar ökar sårbarheten i verksamheten och säkerhetsfrågor blir viktigare. Denna uppsats syftar till att undersöka vilka utmaningar relaterade till informationssäkerhet kan uppstå i samband med digitalisering av HR-processer och hur kan dessa hanteras. En kvalitativ studie genomfördes i form av intervjuer med personer som arbetar med HR och informationssäkerhet. Resultatet visar det finns en medvetenhet kring informationssäkerhet i organisationerna kring mänskliga och tekniska hot och de arbetar aktivt med policys, utbildning och medvetenhet. Men studien identifierar också att informationssäkerhet hamnar inte högst upp på att göra listan, för andra kolliderar säkerhetsfrågorna ofta med verksamhetens bekvämlighet och funktionalitet och dessutom kan det vara kostsamt för alla typer av verksamheter, både att arbeta helt informationssäkert, och att inte göra det alls.

Innehållsförteckning

1	Introduktion	9
1.1	Bakgrund	9
1.2	Problemformulering	10
1.3	Forskningsfråga	10
1.4	Syfte	10
1.5	Avgränsningar	11
2	Litteraturgenomgång	12
2.1	Digitalisering	12
2.2	Human Resources i kontext av digitalisering	13
2.3	Informationssäkerhet	16
2.4	Säkerhetsbrister vid digital HR	17
3	Metod	19
3.1	Metodval	19
3.2	Urval	19
3.3	Intervjuguide	20
3.4	Studiens kvalitet	22
3.5	Transkribering	23
3.6	Analys av data	23
3.7	Metoddiskussion	23
4	Empiri	25
4.1	Intervju	25
4.2	Digitalisering	26
4.3	Human Resources i kontext av digitalisering	27
4.4	Informationssäkerhet	30
4.5	Säkerhetsbrister vid digital HR	33
5	Diskussion	38
5.1	Digitalisering	38
5.2	Human Resources i kontext av digitalisering	38
5.3	Informationssäkerhet	39
5.4	Säkerhetsbrister vid digital HR	40
6	Slutsats	42
6.1	Förslag till fortsatt forskning	42
7	Bilagor	44
	Bilaga A - Transkribering Intervju 1	44

<i>Bilaga B - Transkribering Intervju 2</i>	50
<i>Bilaga C - Transkribering Intervju 3</i>	55
<i>Bilaga D - Transkribering Intervju 4</i>	61
<i>Bilaga E - Transkribering Intervju 5</i>	64
<i>Bilaga F - Transkribering intervju 6</i>	68
<i>Referenser</i>	72

Tabeller

Tabell 1: Definitioner.....	8
Tabell 2: Intervjuguide.....	18

Tabell 1: Definitioner

DDos	Denial-of-serviceattack, en attack som sker där tillåtna användare hindras tillgång till ett datasystem på grund av att en hacker gör upprepade förfrågningar till systemet vilket tar upp systemets resurser (Evans et al., 2021).
Malware	Programvara som är avsedd att göra ett system tillfälligt eller permanent oanvändbart eller att penetrera ett datorsystem helt i syfte att samla in information (Evans et al., 2021).
API	Application programming interface, ett sett rutiner för programvara som tillåter ett system jobba med ett annat (Evans et al., 2021).
Phising	Processen där e-mails skickas ut för att lura internetanvändare att uppge personlig information så som kreditkortsnummer, personnummer och annan känslig information som kan leda till identitets kapning (Evans et al., 2021).

1 Introduktion

Följande kapitel syftar till att ge läsaren en överblick över forskningsämnet. Bakgrunden till arbetet samt problemområdet presenteras här i syfte att visa på ämnets betydelse och behovet av studien. Även studiens forskningsfråga har här formulerats tillsammans med dess syfte och avgränsningar.

1.1 Bakgrund

Svenska företag och organisationer placerar sig generellt i framkant när det gäller digitalisering och digitala verktyg används i allt större utsträckning för att effektivisera processer inom flera delar av organisationerna (Olsson, 2019). Human Resources spelar en viktig roll för organisationernas digitalisering, men HR:s egna digitalisering är minst lika viktig (Ahnlund, 2018).

Digitaliseringen av HR tog fart i samband med införandet av GDPR år 2018. De traditionella tillvägagångssätten att hantera personalinformation och processer uppfyllde sällan GDPR-kraven om rätt till insyn, korrigering och radering av information om de anställda som företaget samlar in och behandlar. Detta bidrog till att organisationer i större omfattning behövde digitalisera sina HR-processer och HR-data (Simpley, 2020). Två år senare deklarerade världshälsoorganisationen WHO Covid-19 som en pandemi (BBC, 2020). Överallt gjorde organisationer och regeringar insatser för att minska smittspridningen. En av dessa var att övergå till distansarbete, vilket i sin tur gav digitaliseringen ytterligare en skjuts och organisationer tvingades att bli digitala snabbt för att tillgodose att de anställda kunde utföra samma arbetsuppgifter som tidigare, men nu digitalt (Europakommissionen, 2020).

Att digitalisera en HR-process handlar inte bara om att göra papper digitala. Det handlar om att tänka kreativt och hur vi på bästa sätt kan effektivisera en process, och samtidigt göra den så enkel som möjligt (Ågren, 2019). Genom att digitalisera mer inom HR frigörs ytterligare tid till organisationsutveckling och människorna i organisationen. Digitaliseringen gör att HR-personalen kan jobba mer med hur företagen är organiserade, vidareutbildning av anställda och samarbete mellan avdelningar. Med en vidare etablerad digitalisering ökar också mängden data och med hjälp av denna kan man inom HR bättre förstå medarbetarnas behov och därmed skapa en bättre arbetsplats (Ahnlund, 2018). Att digitalisera HR kan därför ses som en otrolig möjlighet för organisationer, men ökad digitalisering innebär också ett större behov av informationssäkerhet (Tillväxtverket, 2020).

1.2 Problemformulering

I en undersökning som gjordes av KPMG tillfrågades 1300 HR-ledare runt om i världen om hur framtidens HR-roll skulle se ut. Resultaten visade att en av de största utmaningarna som HR-ledarna ser för framtiden är att förbereda och lära upp sina medarbetare i hur AI och andra liknande teknologier kommer påverka deras roller framöver. Vidare betonar HR-ledarna vikten av att investera i ny HR-teknologi för att öka analysförmågan hos företagen (KPMG, 2020). Undersökningen visar den aktuella utvecklingen av digital-HR och användningen av informationstekniska hjälpmedel i HR-arbetet.

En effekt av digitaliseringen är ökat behov av informationssäkerhet i organisationer. Digitala lösningar ökar sårbarheten i organisationerna och säkerhetsfrågor blir viktigare. För att nyttja fördelarna av digitaliseringen behöver företag ha förmågan att inkludera informationssäkerhetsperspektiven i affärsutvecklingsprocesserna och en integrerad del av verksamheten (Tillväxtverket, 2020).

Idag är IT-system inte bara stöd för organisationerna utan essentiella för att verksamheten ska fungera. Genom att vara medveten om hoten mot systemen kan organisationerna också arbeta för att förebygga dem. Dessa hot kan delas in i tre olika kategorier, mänskliga hot (angrepp, misstag etc.), tekniska hot (systemfel) och naturhot (väderfenomen). Samtliga hot kan leda till incidenter som påverkar informationssäkerheten hos organisationer och i sin tur leda till allvarliga konsekvenser för både individen och organisationerna (MSB, 2021).

1.3 Forskningsfråga

Med den bakgrund som presenterats samt problemformuleringen har nedanstående forskningsfråga formulerats. Forskningsfrågan syftar till att belysa de eventuella utmaningarna gällande informationssäkerhet som uppstår i samband med att HR-arbetet blir alltmer digitalt samt hur organisationer arbetar med att hantera dessa.

”Vilka utmaningar relaterade till informationssäkerhet kan uppstå i samband med digitalisering av HR-processer och hur kan dessa hanteras?”

1.4 Syfte

Syftet med denna studie är att utreda och redogöra för vilka utmaningar som är relaterade till informationssäkerhet som uppstår i samband med att HR-processer i allt större omfattning digitaliseras. Vidare avser studien till att undersöka hur organisationer hanterar dessa utmaningar. Genom att undersöka, återge och analysera litteratur inom ämnet samt intervjua personer som arbetar inom området är ambitionen att få en tydligare förståelse för de utmaningar som finns samt hur organisationer arbetar med att hantera dessa.

1.5 Avgränsningar

För att uppnå syftet med denna uppsats och vidare kunna besvara forskningsfrågan har en avgränsning av uppsatsen varit nödvändig med hänsyn till omfattningen på uppsatsen samt den givna tidsramen. Personerna som intervjuats för studien arbetar alla i organisationer inom privat sektor och därför avgränsas studien till att enbart undersöka hur organisationer inom privat sektor arbetar med informationssäkerhet och HR-digitalisering. Vidare kommer studien inte att behandla verksamheter som enbart arbetar med HR-digitalisering som huvudsyfte utan företag som har identifierat ett behov av att, eller en möjlighet att, digitalisera sina HR-processer i syfte att vidareutveckla sitt arbete inom HR. Avslutningsvis kommer studien inte beröra de hot mot system som klassas som naturhot, då dessa är av mindre relevans i avseende till forskningsfrågan.

2 Litteraturgenomgång

I detta avsnitt utreds begreppet informationssäkerhet samt de modeller som ligger till grund för god informationssäkerhet. I detta avsnitt presenteras också tidigare forskning angående informationssäkerhet kopplat till digitalisering samt Human Resources.

2.1 Digitalisering

Det finns olika definitioner av digitalisering. Digitalisering kan ses som en förändring där det ges nya förutsättningar som följd av teknisk utveckling (SOU 2015:91). Digitalisering kan också ses som en process, där individer och organisationer kan kommunicera och utbyta information på helt nya sätt vilket leder till ökad tillgänglighet och effektivitet (SOU 2016:89).

I litteratur om digitalisering presenteras två begrepp, *digitalization* och *digital transformation*. Dessa två begrepp används synonymt och definieras utifrån ett organisatoriskt perspektiv av Parviainen et al. (2017) som:

“...changes in ways of working, roles, and business offering caused by adoption of digital technologies in an organization, or in the operation environment of the organization.” - (Parviainen et al., 2017, p.64)

Denna studie kommer endast använda begreppet digitalisering och utgå från Parviainens definition ovan, där digitalisering syftar på införandet av ny digital teknik och de förändringar som uppkommer till följd av den implementeringen (Parviainen et al., 2017.)

Digitalisering av organisationer liknas med den transformation som inträffade under industrialiseringen på 1800-talet, när vi gick från jordbrukssamhälle till industrisamhälle. Många kopplar den transformationen till ökad produktivitet men glömmer att det också innebar ökad standardisering. Det samma gäller digitalisering, det kan bidra till ökad produktivitet men också ökad standardisering. Stora skillnaden mellan den tidigare transformationen och den som sker i samband med digitalisering är att den nu påverkar hela verksamheten, inte bara produktionen, det är inte endast ett teknikbyte utan ett förändrat arbetssätt (Börjesson, 2020). I en studie som International Energy Agency (IEA) har genomfört diskuteras risker och fördelar med strukturella transformationer. I studien lyfts säkerhetsrisker i samband med informationssäkerhet och integritet. När det kommer till informationssäkerhet beskrivs det som ju mer digitalt ett system är, desto mer utsatt är systemet för digitalt medförda risker, så som cyberattacker. Vidare tar studien också upp de integritetsfrågor som uppstår när mer och mer detaljerade data samlas in från användarna (Aberge et al. 2017).

Digitalisering påverkar inte bara informationssäkerheten utan förändrar också arbetsplatserna (SOU 2016:85). Det förändrar hur medarbetare förhåller sig till varandra och till organisationen. Idag sker till exempel kommunikation till stor del genom digitala hjälpmedel så som e-mail, Slack och Workplace. Även arbetsplatserna förflyttas från kontor till medarbetarnas egna bostäder eller allmänna platser (Jesuthasan, 2017).

2.2 Human Resources i kontext av digitalisering

Forskare definierar digital HR olika. Enligt Gupta & Saxena (2012) och Bondarouk, Parry och Furtmueller (2017) är digital HR något som genom webbaserade kanaler kan assistera en organisation i att uppnå strategier, policys och praxis. Vidare menar Panayotopoulou et al. (2007) att utbildning av personalen är en avgörande faktor för att implementeringen och användningen av digitala HR-system ska vara lyckat.

2.2.1 Bakgrund

Funktionen Human Resources har under ca 120 år funnits inom svenskt arbetsliv. Under slutet av 1800-talet, när det svenska bondesamhället övergick in i industrialismen och människor flyttade in till städerna, ökade behovet av någon som kunde driva samhällsfrågorna kring hälsa, hygien och levnadsstandarder. I början av 1900-talet kallades rollen personalkonsulent, och började tillsättas på industrierna (Lind, 2020).

Vidare fram mot 60-talet förändrades rollen från att tidigare varit mer en social funktion till att nu innefatta mer personaladministration, lönefrågor samt sociala frågor för de anställda, fackförbunden blir större och arbetsrättslig lagstiftning införs (Lind, 2020).

Det är främst under 2000-talet som digitaliseringen av HR ökat i samband med uppkomsten av Human Resources Information Systems, HRIS. Systemen fokuserar på att samla in och skapa en hållbar digital lösning för att hantera mänskliga resurser (Flynn, 2015). Experter inom HR-området menar att det var dessa HRIS som gav startskottet för det vi idag kallar digital HR och att det var tack vare dessa system som vi nu kunde tillgängliggöra information för hela verksamheten (Lengnick-Hall & Moritz, 2003). Vidare menar Lengnick-Hall & Moritz (2003) att genom att digitalisera HR-funktioner minskade HR-avdelningens administrativa personalarbete (Lengnick-Hall & Moritz, 2003). Denna utveckling har i sin tur bidragit till att möjliggöra ett mer strategiskt HR-arbete för organisationer och HR blir en mer värdeskapande resurs (Som, 2008). Human Resources har under de senaste 30 åren genomgått en transformation. Från att i mitten av 1990-talet arbeta med reaktivt och administrativt till att idag arbeta med proaktivt och värdeskapande i en mer strategisk roll (Findikli & Bayarcelik, 2015).

Det nästa steget för många organisationers HR-medarbetare är nu att arbeta vidare med strategiskt arbete men övergå mer digitalt med hjälp av digitala HR-system, så kallat e-HRM, Electronic Human Resources Management (Stone et al., 2015). e-HRM är ett resultat av implementering av informationsteknologiska lösningar som ett verktyg för Human Resources Management, likt den teknologiska utvecklingen som också skett inom andra områden så som ekonomi och marknadsföring (Ulrich and Dulebohn, 2015).

2.2.2 Digitalisering av HR funktioner

Digital HR har utvecklats i syfte att generera en värdefull informationsdatabas över de mänskliga resurserna i en organisation. Digital-HR är idag ett övergripande paraply-begrepp som innefattar många olika digitala HR-verktyg (Gupta & Saxena, 2012). Dessa olika verktyg kan tillsammans skapa ett övergripande HR-system, ett e-HRM, där de olika verktygen kan integrera med varandra (Stone et al., 2015).

E-recruitment (e-rekrytering)

E-rekrytering omfattar rekrytering och urval. E-rekrytering innefattar också jobbportaler exempelvis LinkedIn, och personlighetstester (Brahamana & Brahamana, 2013).

E-learning (e-lärande)

E-lärande är ett samlingsnamn för verktyg som används för att utbilda och utveckla medarbetare. Även karriärs-planering och internet-källor för online utbildning innefattas av e-lärande. E-lärande innebär även möjligheter för varje anställd att kontrollera och följa upp sin egen inläring. Det finns många fördelar för en organisation att använda sig av e-lärande, framför allt ökad tillgänglighet av utbildning för medarbetarna och billigare kompetensförsörjning (Navimipour & Zareie, 2015).

E-Communication (digital kommunikation)

Digital kommunikation syftar till de digitala verktyg som används för att kommunicera på arbetsplatser, där E-mail är den vanligaste formen av kommunikation. Vidare är också intranät, snabbmeddelanden och olika former av e-forum en del av en organisations digitala kommunikation. Generellt ska systemen kunna förmedla information och kunskap inom organisationen, både från chefer och ut i organisationen och tvärt om (Gupta & Saxena, 2012).

Planning e-HR (digital personalplanering)

Digital personalplanering syftar till skapandet av databaser med personaluppgifter i form av avtal, arbetsförutsättningar och personliga data. Systemen baseras ofta på självservice och tillåter medarbetarna själva uppdatera informationen. De kontinuerliga uppdateringarna av systemet tillhandahåller uppdaterade data och information till chefer och HR-avdelningen (Panayotopoulou et al., 2007). Systemet ger också unika stödsystem till medarbetarna i organisationen och möjliggör decentraliserade beslut (Gupta & Saxena, 2012).

Rewarding e-HR (digitala belöningsystem)

Digitala belöningsystem består av system för utvärdering, ersättning och förmåner. Systemen innefattar målsättning, prestationsmätning och ansvarsfördelning och tillåter de anställda att själva kunna tillhandahålla preferenser kring sitt arbete så som lön och förmåner. Detta fungerar sedan som beslutsunderlag för chefer huruvida till exempel bonusar ska betalas ut och ständigt utvärdera arbetet som sker (Panayotopoulou et al., 2007).

Performance e-HR (prestationsutvärdering)

Performance e-HR är performance managementsystem som för samman kunskap, färdigheter och kompetens som påverkar de anställdas prestationer. Verktyg för prestationsutveckling syftar till att öka kunskapen kring och om de anställdas individuella prestationer genom olika mätverktyg. Den data kan sedan användas vid mål- och medarbetarsamtal (Tomic, Tadic & Sedlak, 2016).

Protecting e-HR (digitala system för säkerhetsfrågor)

Digitala system för säkerhetsfrågor samlar information om juridiska frågor, hälsa, relationer och säkerhetsverktyg och gör informationen tillgänglig för chefer och anställda. Genom verktyget kan chefer kontinuerligt uppdateras kring risker i organisationen Findikli och Bayarcelik (2015).

2.2.3 Användning av Artificiell Intelligens i digital-HR

Genom att digitalisera flera delar inom HR genereras stora mängder data (big data) och feedbackloops vilket möjliggör användningen av artificiell intelligens. Idag är det möjligt att använda tillgängliga data i form av CV, jobbprofiler och LinkedIn tillsammans med algoritmer för att göra en urvalsprocess som motsvarar en professionell rekryterares och genom maskininlärning blir dessa algoritmer bättre och bättre, det enda som behövs är ständig feedback. Vidare skapar en anställd och lämnar efter sig data i nästan allt de gör i arbetet, transaktioner, kommunikation, klick, nedladdningar och användning av olika plattformar, och den data kan sedan i sin tur användas för att optimera de system och den miljö de anställda arbetar i. Det finns flera sammanhang där Artificiell Intelligens (AI) kommer till användning i en HR-kontext (Trost, 2020). Följande är några sammanhang där AI kommer till användning samt hur AI används i dessa:

Lärande och användningen av resurser för lärande: Baserat på medarbetarens tidigare inlärningsbeteenden och dess användning av tidigare resurser, arbete, projekt och sociala relationer till kollegor kan algoritmen föreslå utbildningar för medarbetaren på relevant lärandeplattform. AI kan även rekommendera vem i organisationen en anställd kan prata med för ett direkt personligt utbyte för att lära av varandra (Trost, 2020).

Kandidatsökning, rekommendationer och kandidaturval: Med grund i den data som finns tillgängligt online om kandidater, söks och föreslås kandidater utifrån nuvarande arbetsbehov. Med hjälp av maskininlärning kan man också söka efter kandidater som är lämpliga baserat på andra faktorer än de som de själva presenterar på till exempel LinkedIn. Jobbsökande kan få automatiska platsannonser utifrån sitt nätverk och egenskaper, ett så kallat rekommendationssystem och det samma gäller urvalet av kandidater och sökande. Systemen screenar och utvärderar inkommande Cv:n med hjälp av självoptimerande algoritmer (Trost, 2020).

Chatbottar: Sökande och kandidater kan kommunicera med ett dialogbaserat system och kan därför få svar i realtid på frågor. Dessa system kan i större utsträckning anpassa sig till mottagarens humör och föredragna kommunikationsstil (Trost, 2020).

Prestationsmätning, lojalitetsmätning och talangidentifiering: Företag kan med hjälp av transaktionsdata, kommunikation, närvaro och frånvaro, förutsäga framtida prestationer och lojalitet till företaget. Utifrån detta kan företagen identifiera vilka anställda som vill utvecklas internt och vilka som kan vara på väg att sluta. Vidare kan företagen med hjälp av data, algoritmer och maskinintelligens identifiera talanger, så kallad digital talent identification. Detta genom att endast några få indikatorer som behöver viktas och kombineras därefter (Trost, 2020).

Organisation: Inom idrotten är det idag möjligt att analysera data kring rörelse, interaktion och prestation för att förutsäga vilken lagkonstellation och vilket samspel är mest optimalt för vilken motståndare. Dessa metoder är även applicerbara i entreprenörssammanhang för att para ihop framgångsrika samarbetskonstellationer (Trost, 2020).

2.3 Informationssäkerhet

Informationssäkerhet syftar till att skydda informationstillgångar som lagras, bearbetas eller överförs med hjälp av policys, utbildning, träning, medvetenhet och teknologi (Whitman & Mattord, 2011). Whitman & Mattord (2011) vidare definierar informationssäkerhet som skydd av information och dess kritiska element. Detta inkluderar de system och den hårdvara som använder, lagrar och överför den informationen. Varje komponent har olika säkerhetshot som behöver adresseras. Informationssäkerhet handlar om att bibehålla och skydda integriteten, tillgängligheten och sekretessen av dessa komponenter (Whitman & Mattord, 2011). En vanlig modell för att förklara informationssäkerhet är CIA-triaden (se nedan).

2.3.1 CIA-triaden

Grunden till informationssäkerhet och alla säkerhetsprogram förkroppsligas av tre komponenter; confidentiality, integrity och availability. Tillsammans formar de en erkänd modell inom informationssäkerhet som kallas CIA-triaden. CIA-triaden används som guide för informationssäkerhetspolicys i privata och offentliga organisationer och är också grunden till säkerhetsprogram (Stallings & Brown, 2018).

Confidentiality (konfidentialitet) är den första komponenten i CIA-triaden. Termen konfidentialitet kan liknas vid sekretess och beskrivs som att skydda data från obehörigas åtkomst och missbruk. Genom att vidta åtgärder för att säkerställa konfidentialitet förhindras att känslig information når fel personer, men också att säkerställa att rätt personer också har tillgång till den. Exempel på sådana åtgärder är åtkomstkontroller, datakryptering, löpande övervakning, testande och utbildande av personal (Möller, 2020). Personal på företag ombeds ofta ha svårgissade inloggningsuppgifter, vilket är ett konkret exempel på hur företag arbetar med konfidentialitet.

Integrity (integritet) är den andra komponenten i CIA-triaden. Integritet handlar om att upprätthålla korrekt och komplett data, samt att denna är tillförlitlig och inte ändrats av icke auktoriserade användare eller processer (Wylder, 2003). Komponentens integritet berör både systemintegritet och dataintegritet. Systemintegritet syftar till kravet på att ett system ska utföra sin avsedda funktion på ett opåverkat sätt, fritt från uppsåtlig eller ouppsåtlig otillåten manipulation. Dataintegritet syftar till kravet på att data och program bara ska kunna ändras på ett specificerat och auktoriserat sätt. Brist på integritet möjliggör modifiering av data vilket kan påverka avgörande och kritiska funktioner i de operativa funktionerna i digitala system (Möller, 2020).

Availability (tillgänglighet) är den sista av de tre komponenterna i CIA-triaden. Den syftar till att information, data och program ska vara tillgängligt och aktuell för behöriga användare när det behövs. Detta säkerställs genom konstant underhåll, uppdatering och reparationer av nätverks säkerhet och systemhårdvara samt upprätthållande av en korrekt, fungerande, operativ systemmiljö (Möller, 2020). Exempel på när tillgängligheten blir begränsad är nätverksfel, systemfel och strömavbrott, dessa bidrar till att informationen inte blir tillgänglig för användaren (Andress, 2014).

2.4 Säkerhetsbrister vid digital HR

I samband med att HR digitaliseras genereras en stor mängd data inom organisationerna. Det innebär att det tillkommer nya svårigheter, bland annat att garantera denna datas säkerhet. HR-systemen förvarar personnummer, löner, prestationsdata och medicinsk historia. Detta är information som anses varas konfidentiell och riskeras att avslöjas, avsiktligt av en missnöjd anställd, eller oavsiktligt av någon som inte fått rätt utbildning i användningen av digitala HR-system. Informationen kan också ändras eller förvanskas. Alla dessa säkerhetshot kan påverka en organisation negativt och leda till skadliga konsekvenser för verksamheten så som förlust av affärer, stämningar eller konkurs (Townsend & Bennett, 2003).

Enligt Myndigheten för säkerhet och beredskap (2021), kan hot mot system delas in i tre övergripande kategorier, naturhot, tekniska hot och mänskliga hot. Samtliga hot kan leda till incidenter som påverkar informationssäkerheten hos organisationer och i sin tur leda till allvarliga konsekvenser för både individen och organisationen (MSB, 2021).

2.4.1 Tekniska Hot

Som nämnt ovan är en av de stora tekniska säkerhetsriskerna med HR-system är att de innehåller stora mängder data. GDPR, den allmänna dataskyddsförordningen, infördes 2018 och ställer höga krav på hur organisationer behandlar sina anställdas personuppgifter men även kunders och blivande medarbetares. Om en obehörig får tillgång till dessa kan det inte bara innebära konsekvenser för verksamheten utan också innebära hög risk för den enskilde (Lillkrona, 2022). Exempelvis så kan avslöjandet om sådan personlig information komma att påverka vid en befordran eller leda till att bli nekad en anställning (Zafar, 2013). Exempel på sådana tekniska hot som kan påverka en organisations informationssäkerhet är cyberattacker. Cyberattacker görs av hackare för att stjäla data, infektera datorer eller ta kontroll över datorer, system och nätverk. Det finns flera olika typer av skadliga programvara som används av hackare för att skada systemen, virus, ransomware, scareware, trojaner etc. (Evans et al., 2021).

Att erbjuda HR-system som molntjänster är en affärsmodell som blir alltmer populär i organisationerna. Detta innebär ytterligare en säkerhetsrisk för verksamheten. Molntjänster, eller Cloud computing, är ett samlingsbegrepp för hård- och mjukvarutjänster som levereras över nätverk till kund med hjälp av självbetjäning och är oberoende av plats och enhet (Liu et al., 2018).

I samband med att mer information om personer och verksamheter lagras i molntjänster, ökar oron för hur säker molnmiljön faktisk är (Popović & Hocenski, 2010). Verksamheter som förvarar data i molntjänster riskerar att möta utmaningar som är större än i traditionella system (Armbrust et al., 2010; Chow et al., 2009) och som inte heller kan bemötas med samma traditionella medel som andra informationssäkerhetsutmaningar (Zissis & Lekkas, 2012). Data-och nätverksintrång, malware-injektioner, osäkra API: er, DDoS-attacker, sårbarheter i systemen och phishingattacker är bara några av de utmaningar som omnämns (Rizwan & Zubair, 2019).

2.4.2 *Mänskliga hot och mänsklig faktor*

En av de främsta anledningarna till säkerhetsbrister och incidenter är människor och den mänskliga faktorn (Skrodelis, Strebko & Romanovs, 2020). Till den mänskliga faktor räknas samtliga misstag eller fel som en människa gör, oavsett om de sker med medvetenhet eller omedvetenhet och med ond avsikt eller i god tro (Kraemer & Carayon, 2007).

Kremaer och Carayons (2007) studie visade att många fel som sker på grund av mänsklig faktor är relaterade till organisatoriska faktorer. Ofta är de relaterade till organisationens kommunikation, säkerhetskultur eller säkerhetspolicy (Kraemer & Carayon, 2007). Exempel på sådana misstag är att glömma byta lösenord, glömma logga ut när man lämnar datorn eller att hantera information oförsiktigt (Warkentin & Willison, 2009). Det är svårt att helt undvika den mänskliga faktorn, men det finns faktorer som kan leda till att antalet fel som uppstår på grund av den mänskliga faktorn, minskar (Wood & Banks, 1993). En av de främsta åtgärderna för att minska antal misstag som sker på grund av den mänskliga faktorn är att skapa en medvetenhet hos de anställda. Denna medvetenhet skapas genom utbildning och träning inom området. Utbildningen ska öka förståelsen hos användarna och öka medvetenheten kring riskernas omfattning (Siponen, 2000). Ett sätt att göra detta är genom att tillhandahålla en säkerhetspolicy. En säkerhetspolicy är riktlinjer som anställda förväntas följa för att bibehålla ett säkert arbetssätt (Alotaibi, Furnell & Clarke, 2019).

3 Metod

I detta avsnitt presenteras vald metod för studien. Vidare redogörs det för hur datainsamling genomfördes i form av en litteratursökning och intervjuer. Avslutningsvis diskuteras även etik, reliabilitet och validitet i samband med studien.

3.1 Metodval

För att uppnå syftet med denna studie krävs det att relevant metod används. Den metod som används i denna studie är kvalitativ. Efterforskningens resultat har utgångspunkt i erfarenheter från ett flertal respondenter. Den kvalitativa metoden tillåter djupare perspektiv från respondenterna då de ger möjlighet och utrymme för mer nyanserade, detaljerade svar och förtydliganden. Kvalitativa intervjuer ger också ofta deskriptiva svar på frågor som *hur?* och *varför?* (Rienecker & Stray Jörgensen, 2014). Kvalitativa studier anses dessutom vara passande för forskning som syftar till att besvara explorativa frågeställningar Jacobsen (2002). Något denna studie kan anses vara.

För att besvara forskningsfrågan om vilka utmaningar gällande informationssäkerhet som uppkommer när man digitaliserar HR-processer började arbetet inledningsvis med en litteraturstudie. Syftet med litteraturstudien var att få en bredare inblick i vad tidigare forskning inom ämnet funnit samt att få djupare kunskap inom området. För att hitta relevant forskning, publikationer och litteratur på ämnet användes LUBSearch samt Google Scholar. Även vanliga Google sökningar har används för att finna artiklar inom ämnet. Sökord som använts i alla sökmotorer har bland annat varit:

"HR-digitalisering", "Digitalisering HR-processer", "informationssäkerhet HR", "Informationsecurity HR", "HR-digitalisation", "HR-digital transformation"

Sökningarna gjordes både på svenska och engelska för att få ett bredare utbud av information till insamlingen.

Därefter genomfördes kvalitativa intervjuer med representanter från företag som har identifierat ett behov av att, eller en möjlighet att, digitalisera sina HR-processer i syfte att vidareutveckla sitt arbete inom HR eller arbetar med digitalisering. Kvalitativa intervjuer ger insikt om intervjupersonernas egna erfarenheter, tankar och känslor (Dalen, 2015). Vidare kom intervjuerna att genomföras efter en semistrukturerad modell. Semistrukturerade ger intervjupersonerna möjlighet att utforma svaren på eget sätt och frågorna är öppet formulerade och kan kompletteras med följdfrågor från intervjuaren (Bryman, 2018).

3.2 Urval

I ett initialt skede av urvalsprocessen gick arbetet ut på att skaffa en överblick över möjliga informanter. Under den processen utvecklades avgränsningar för studien och utifrån dessa kunde sedan kriterier för studiens informanter utformas (Jacobsen, 2002). Tidigt definierades ett möjligt hinder i att yrkesverksamma inom HR möjligtvis inte innehar den kunskap som

krävs för att diskutera informationssäkerhet, därför eftersöktes informanter som kunde fördelas i två olika grupper, och då uppfyllde två olika kriterier. Den ena gruppen av informanter uppfyller följande två kriterier:

- Arbetar i en HR roll
- Arbetar med digitalisering

Den andra gruppen av informanter uppfyller följande kriterier:

- Arbetar med informationssäkerhet
- Arbetar eller har arbetat i en organisation som arbetar med HR och har därför insikt i HR-arbetet

För att finna informanter som uppfyllde kriterierna utgick jag i första hand utifrån ett bekvämlighetsurval, vilket innebär att intervjuerna sker med personer som är bekanta. Vidare kallas det snöbollsurval när bekanta hänvisar till andra personer (Jacobsen, 2002). Genom att dela ett inlägg på LinkedIn nådde jag ut i mitt professionella kontaktnät och med hjälp av det fick jag kontakt med flera lämpliga kontakter som antingen själva var intresserade av att ställa upp i intervjun eller kunde rekommendera en kollega eller en annan kontakt att kontakta. Därför består urvalet till denna studie både av personer från ett bekvämlighetsurval samt snöbollsurval.

3.3 Intervjuguide

Intervjuerna för studien följde samma struktur uppdelat i fem övergripande områden. Varje område inkluderade ett visst antal förbestämda frågor. Nedan följer en förenklad översikt över intervjuguiden.

Tabell 2: Intervjuguide

Kategori	Beskrivning	Frågor
Introduktion	Börja med att tacka för deltagandet. Kort presentation av vem jag är samt informera intervjupersonen om de etiska riktlinjer som intervjun och studien tar hänsyn till samt intervjupersonens rättighet att granska intervjumaterialet innan det publiceras.	
Bakgrund	Generella frågor kring intervjupersonens bakgrund, om arbetsroll, om organisationen.	<ol style="list-style-type: none"> Vilken är din roll på företaget och vilket arbetsområde är du verksam inom? Skulle du kortfattat kunna beskriva ert företag? Vilken bransch tillhör ni?

<p>Digitalisering</p>	<p>Undersök i vilken utsträckning organisationen arbetar med digitalisering av HR-processer. Hur intervjupersonen förhåller sig till digitalisering och vilken digital kompetens personen har.</p>	<ul style="list-style-type: none"> a. Hur arbetar ni med digitalisering på din arbetsplats? <ul style="list-style-type: none"> a. Hur har digitalisering påverkat din roll och dina arbetsuppgifter? b. Vilka utmaningar ser du med digitaliseringen? c. Vad innebär begreppet digital HR för dig? d. Vad använder du för digitala HR-verktyg i ditt arbete? / på din arbetsplats? e. Hur behandlas schema, lön, önskemål om ledighet osv? f. Skulle du anse att du har tillräcklig kompetens för att hantera digitaliseringen inom HR? <ul style="list-style-type: none"> a. Skulle du säga att er HR-avdelning har kompetens inom området? b. Har din HR-avdelning fått någon utbildning inom området?
<p>Informationssäkerhet</p>	<p>Undersök hur organisationen arbetar med informationssäkerhet, vilken kompetens intervjupersonen och HR-avdelningen har inom ämnet och vidare vilka informationssäkerhetsutmaningar som personen kan identifiera i sin organisation.</p>	<ul style="list-style-type: none"> a. Hur arbetar ni med informationssäkerhet på din arbetsplats? b. Har ni en informationssäkerhetspolicy eller en informationssäkerhetsstrategi? <ul style="list-style-type: none"> a. Om ja, Hur ser arbetet ut för att etablera den? c. Brukar ni genomföra riskanalyser? d. Hur arbetar du med informationssäkerhet i din roll? e. Hur arbetar ni med att skapa medvetenhet kring informationssäkerhet på din arbetsplats? f. Har du någon särskild kunskap/utbildning inom informationssäkerhet? <ul style="list-style-type: none"> a. Om ja, vad för utbildning? g. Har ni fått någon specifik utbildning i hur ni ska arbeta med informationssäkerhet just i din roll? <ul style="list-style-type: none"> a. Om ja, kan du berätta mer om hur den sett ut? b. Är det något som uppdateras? h. Vilka utmaningar ser du med hur ni arbetar med digitalisering kopplat till informationssäkerhet? i. Upplever ni att det finns en risk eller utmaning med att obehöriga får tillgång till känsliga data i samband med att man digitaliserar stora delar av HR-processerna? <ul style="list-style-type: none"> a. Om ja, hur hanterar ni den risken?
<p>Avslutning</p>	<p>Avsluta med en fri diskussion där intervjupersonen har möjlighet att göra tillägg för att komplettera tidigare diskussion. Tacka för deltagande och avsluta intervjun.</p>	<ul style="list-style-type: none"> a. Finns det något du vill tillägga kring ämnet och det vi diskuterat?

3.4 Studiens kvalitet

3.4.1 Validitet och reliabilitet

Validitet och reliabilitet används för att bedöma kvaliteten på den data som samlas och mäter faktorer så som empirins tillförlitlighet, trovärdighet och giltighet (Jacobsen, 2002).

Studiens validitet syftar till huruvida mätvärdet för undersökningen stämmer överens med det som det är avsett att mäta. Detta kan förklaras så som relevansen av den insamlade data för det givna problemet. För att data ska ha validitet, bör datainsamlingen samt bearbetningen av data utförts korrekt samt att data överförts och dokumenterats korrekt. Avslutningsvis måste den insamlade data vara av relevans för utredningen (Alvehus, 2016).

Studiens reliabilitet syftar till att på ett intressant, pålitligt och begripligt sätt beskriva hur studien har gått till väga för att samla in och bearbeta data. Reliabilitet är av högre relevans vid kvantitativa studier, då reliabilitet i kvantitativa sammanhang syftar till att kunna beskriva hur datainsamlingen skett, för att liknande resultat ska kunna uppstå vid upprepad mätning. För denna studie har datainsamlingen vid samtliga intervjuer skett digitalt i liknande miljöer samt att intervjuerna har utgått från samma intervjuguide (Jacobsen, 2002).

3.4.2 Generaliserbarhet

Generaliserbarhet, benämns ibland som extern validitet eller överförbarhet, och hänvisar till möjligheten att tillämpa studiens resultat på andra exempel av händelsen. Att studien har en förmåga att förklara, eller förekomma i liknande företeelser. För att kunna mäta en studies generaliserbarhet krävs det att material tillhandahålls för att andra ska kunna jämföra studien (Denscombe, 2009). I denna studie presenteras intervjumaterialet och en tydlig avgränsning är gjord för att visa på vart studien kan anses vara applicerbar och då resultatet överförbart inom.

3.4.3 Etik

För att säkerställa en etiskt korrekt intervjuprocess har intervjuerna utgått ifrån tre etiska grundkrav, informerat samtycke, krav på privatliv samt krav på att bli korrekt återgiven (Jacobsen, 2002).

Kravet om informerat samtycke uppfylls genom att intervjupersonerna dels deltar frivilligt i intervjun ges möjligheten att vidare inte delta i intervjun, dels att de har blivit tillfrågade om samtycke för att spela in intervjun för transkribering samt samtycke till att använda det empiriska material som samlats in under intervjun till studien. Vidare har intervjupersonerna i tidigt skede fått information om syftet för intervjun samt vad intervjun kommer att handla om.

Fortsättningsvis uppfylls kravet om rätt till privatliv genom att all insamlade data kommer anonymiseras, samt att alla kommer erbjudas att förbi anonyma. Då företags hantering av informationssäkerhet kan anses som känslig information kommer även verksamheterna

anonymiseras samt att beskrivningarna av verksamheterna kommer generaliseras så de ej går att identifiera i efterhand. Av samma anledning har vissa stycken i transkriberingen tagits bort för att inte kunna härleda transkriberingen av intervjuerna till intervjuperson eller organisation.

Slutligen för att uppfylla kravet på att bli korrekt återgiven kommer intervjuerna spelas in för att få en korrekt transkribering av intervjuerna, därefter skickades transkriberingen till intervjupersonen i fråga för att ge dem möjlighet att invända om något inte stämmer. Detta möjliggör också intervjupersonerna att korrigera intervjun om de anser att information som uppgetts är känslig och inte bör vara med i transkriberingen (Oates, 2005).

3.5 Transkribering

För att underlätta analys av det empiriska materialet spelades samtliga intervjuer in. Att transkribera det inspelade materialet underlättar analys av materialet då det formaterats till skriftlig form (Oates, 2006). Intervjuerna genomfördes över en veckas tid och transkriberingen av dessa gjordes löpande i närtid till genomförandet av respektive intervju. Vid transkribering av de inspelade intervjuerna har utfyllnadsord och dylikt tagits bort och materialet har anonymiserats. Samtliga intervjuer genomfördes digitalt vilket har inneburit ett fåtal tekniska störningar på inspelningarna, dessa har också uteslutits från transkriberingen då de inte ger något värde till studiens resultat. Avslutningsvis skickades transkriberingen till intervjupersonen ifall de skulle önska att ändra något i texten.

3.6 Analys av data

Processen att analysera kvalitativa data innefattar oftast fem steg, förberedelse av data, förtrogenhet med data, tolkning av data, verifiering av data och presentation av data. I första steget, förberedelse av data, har intervjuerna spelats in och sedan transkriberats. För att inte riskera att gå miste om något data har inspelningen av intervjun och transkriberingen inte förvarats på samma plats. I nästa steg, förtrogenhet med data, har intervjuernas transkriberingar lästs igenom vidare har materialet bearbetats återkommande vid flera tillfällen. För att sedan i ett tredje steg tolka data kategoriserats utifrån samma mall som litteraturstudierna. De delar av intervjupersonernas svar som inte faller inom ramarna för uppsatsens undersökning har inte redovisats i empirin, då de bedöms som irrelevant för att kunna besvara forskningsfrågan. Vidare har data verifierats enligt ovanstående punkter (3.4), validitet, reliabilitet, generaliserbarhet och etik. Slutligen presenteras data i nedanstående kapitel, empiri (Denscombe, 2009).

3.7 Metoddiskussion

Vid utförandet av de semistrukturerade intervjuerna spelades intervjuerna in efter godkännande av respondenten. Enligt Bryman (2018) kan medvetenheten kring att en intervju spelas in och att denne blir observerad, leda till reaktiva effekter (Bryman, 2018). Detta var dock inget som upplevdes, ingen av respondenterna hade någon kommentar kring att bli

inspelad och fördelarna med att i efterhand kunna transkribera intervjuerna, övervägde risken för att inspelningen skulle komma att påverka intervjun.

Ytterligare något som kan ha påverkat och kom att reflekteras i intervjupersonernas svar var den arbetsroll de hade. Över lag anser jag att det gav en positiv insikt i hur olika personer som arbetar i någorlunda samma kontext ser på utmaningar inom ramarna för uppsatsens problemformulering. Även om intervjuerna utgick från samma mall var det svårt för respondenterna att svara på alla frågor, beroende på vilken arbetsroll de har. Detta har i sin tur påverkat hur svaren kan jämföras med varandra. Därför tror jag att det hade underlättat om det hade gjorts en avgränsning till en viss HR-roll eller informationssäkerhets-roll. Dock anser jag att bredden av arbetsroller har bidragit till ett bredare perspektiv hur informationssäkerhet i relation till HR-processer hanteras i olika organisationer.

4 Empiri

I detta avsnitt presenteras resultatet från intervjuerna. Inledningsvis kommer de organisationer och respondenter som medverkat i studien presentera. Vidare följer en redogörelse över det empiriska resultatet kategoriserat i samma format som litteraturstudierna i fyra underavsnitt: digitalisering, Human Resources i kontext av digitalisering, informationssäkerhet och säkerhetsbrister vid digital HR.

4.1 Intervju

Som redogjorts för i tidigare metodavsnitt presenteras de olika respondenterna anonymt. Nedan följer en kortare beskrivning av dem.

Intervjuperson 1 - Intervjuperson 1 arbetar för en stiftelse med cirka 350 anställda och arbetar bland annat med omställningar. Intervjuperson 1 är informationssäkerhetsansvarig för stiftelsen och dess dotterbolag. Rollen tillhör organisatoriskt HR avdelningen. Intervjuperson 1 refereras till som I:1.

Intervjuperson 2 - Intervjuperson 2 arbetar på ett mindre företag inom Human Resources som är i start-up fasen med cirka 20 anställda. Verksamheten arbetar dels med search rekrytering och med HR konsulter som går in för att förstärka HR grupper på företag bland annat inom digitalisering av HR. Intervjuperson 2 är VD för företaget och arbetar även som senior HR Tech konsult samt konsultchef. Intervjuperson 2 refereras till som I:2.

Intervjuperson 3 - Intervjuperson 3 arbetar inom en större koncern i service-branschen som är verksam i flera länder. Koncernen har ett tiotusental anställda. Intervjuperson 3 arbetar som HRIS specialist för företagets HR-plattform och arbetar med att ta hand om systemet, utveckla, förvalta och delta i hela digitaliserings processen. Intervjuperson 3 refereras till som I:3.

Intervjuperson 4 - Intervjuperson 4 arbetar inom en decentraliserad organisation som är verksam inom bank och försäkring. Organisationen har strax under 10 000 anställda. Intervjuperson 4 arbetar i en roll inom HR och är förvaltningsansvarig för organisationens HR-IT system. Intervjuperson 4 refereras till som I:4.

Intervjuperson 5 - Intervjuperson 5 arbetar som HR konsult ute i olika företag med HR processer och HR-transformation. Tidigare arbetade intervjuperson som Global Head of HR-operations på ett stort amerikanskt företag med omkring 55 000 anställda. Där arbetade intervjuperson 5 med att utforma en global HR-teknologistrategi, implementering av HR-system, men också roles and responsibilities, HR-processer och HR-datasäkerhet. Intervjuperson 5 refereras till som I:5.

Intervjuperson 6 - Intervjuperson 6 arbetar som serieentreprenör och har de senaste 20 åren arbetat med att bygga och utveckla bolag inom cybersäkerhet. Intervjuperson 6 refereras till som I:6.

4.2 Digitalisering

Empirin visar att organisationerna arbetar med digitalisering på olika sätt och i olika omfattning. Intervjuperson 1 beskriver hur dem i deras organisation har digitalisering som en del av DNAt och att den digitala strategin, där digitalisering ingår, är en del av organisationens verksamhetsstrategi och att dem idag arbetar med att erbjuda alla deras tjänster digitalt.

”Digitalisering är egentligen en del av DNAt... Så digitaliseringen är a och o, den är primär, det innebär att rent konkret att alla tjänster som vi idag erbjuder fysisk eller har erbjudit fysiskt ska kunna erbjudas digitalt och det primära utvecklingsområdet egentligen är att vi utvecklar våra tjänster och funktioner så allt ska kunna vara tillgängligt digitalt.” – I:1, 2022

Även Intervjuperson 3 diskuterar digitalisering som en självklar del av organisationen och ett pågående projekt där man idag gör nästan allt digitalt genom system, appar och digitala verktyg men också ser över organisationens processer.

”Så det är titta på den här resan med alla delar som finns det och se till att det görs genom digitala verktyg och automatisera processen om det är möjligt och sen också titta på vad företaget behöver från HR som organisation också ser till att det inte görs på papper, det görs digitalt och det vi gör det inte digitalt för att det är kul att göra det digitalt bara. Tänk på att jag kanske inte alls arbetat med papper i sådana steg de senaste åren, eller jag behövde inte arbeta med papper så här sällan, man gör allt genom system, appar och digitala verktyg.” – I:3, 2022

Upplevelsen kring hur digitalisering mottas i organisationerna är liknande hos alla intervjupersonerna och de alla vittnar om att det är en blandad reaktion ute i organisationerna. Intervjuperson 5 beskriver mottagandet från organisationerna som optimistiskt och lite naivt, där många ser det som att IT-system löser allt men inte förstår att implementeringen i vissa fall kan innebära mer arbete.

”... man tittar på det ganska optimistiskt, men tänker man ser inte, ja man tänker att IT-system löser ting, och så tänker man att det går ganska lätt och att man inte behöver göra något jobb själv. Så i första omgång blir det mottaget ganska positivt och man tänker, jaja, IT systemen löser det, men så har man implementerat det, och så finner man ut att man at man inte är self-service och så vidare, det fungerar inte om man inte tänkt på hur man ska göra det. Så i första omgången är man väldigt optimistisk och kanske lite naiv, och i andra omgången blir man så förtvivlad eller skuffet över den upplevelse som man har.” – I:5, 2022

Intervjuperson 4 betonar vikten av att skapa en förståelse för varför man genomför en förändring i organisationen och beskriver att om medarbetarna får ett stöd som är bättre än tidigare och underlättar vardagen, samt en förståelse för att somliga rutiner kommer förändras så välkomnas mottagandet väl.

”...jag skulle säga att mottagaren av det, så länge dom får ett stöd som är bättre än vad de haft innan och de förstår varför de kanske måste ändra vissa rutiner så

skulle jag säga att mottagandet välkomnas och allt som gör din vardag lättare och det är ju det som är syftet.” – I:4, 2022

Detta styrks av Intervjuperson 1:

”...alla behöver olika tid på sig, så det tas emot väl, och det hela handlar om att paketera värde, alltså nyttorealiserings liksom, varför gör vi det här, vare sig det handlar om inköp av nytt system att säkra upp nya processer, varför gör vi det. Jag tror när du paketerar det bra och jobbar med kulturen och acceptansen, då tas det emot på mycket bättre sätt än att du ska bara slänga ut system och så säger någon nu ska du använda det här för att det funkar sällan bra”- I:1, 2022

Något som tas upp av flera intervjupersoner är också vikten av att ha en ledning i organisationen som är drivande i frågan kring att digitalisera. Intervjuperson 1 visar ett tydligt exempel i när organisationen fick en ny chef med intresset för digitalisering vilket förändrade organisationens sätt att arbeta med digitalisering.

”...4–5 år sedan, så var inte digitaliseringen inte en del av organisationens dna men sen fick vi en nyhet till chef som satte det som en digital strategi, som är parallell med alla andra strategier bara för att liksom komma in i second phase, en andra andning, och sen blev den digitala strategin är en del av vår huvudstrategi, verksamhetsstrategi helt enkelt.” – I:1, 2022

Detta stöds av intervjuperson 3 som anser att det är viktigt i en organisation att management, ledningen, oavsett nivå, har en positiv inställning mot digitalisering och menar att om de som fattar beslut i organisationen inte vill digitalisera är det svårt att motivera resten av organisationen också.

”...men det som är viktig i en organisation är att management, de som fattar beslut, oavsett i vilken nivå, har ett positivt tankar mot digitalisering. Om de som fattar beslut vill inte digitalisera eller att rädda från digitalisering det finns det svårt och övertyga.” – I:3, 2022

4.3 Human Resources i kontext av digitalisering

I frågan gällande begreppet digital-HR och dess innebörd har intervjupersonerna alla liknande uppfattningar kring vad begreppet innebär. Automatiserade processer och att ge tjänster inom HR på ett digitalt sätt är två av definitionerna som lyfts i intervjuerna.

”...det är dels att det är vissa processer som är automatiserade som man inte längre gör som man gjorde tidigare. Jag tänker också att det finns en annan nivå där man kanske digitaliserar genom att flytta vissa arbetsuppgifter till ett annat verktyg så att det inte blir automatiserat men man jobbar i andra verktyg för att utföra det” – I:2, 2022

”det om att göra, att ge en HR tjänst till företaget som organisation och till anställda som behöver tjänster från HR på ett digitalt sätt, och när man säger digitalt sätt det är inte bara att använda ett digitalt verktyg. digitala verktyg, det innebär att vi levererar på ett snabbt effektivt kommunikativt sätt som når alla och som gör det lätt.” – I:3, 2022

Samtliga intervjupersoner använder digitala HR-verktyg i sitt arbete i större eller mindre utsträckning. De större organisationerna använder sig av flera digitala HR-verktyg och fler digitala system i organisationen än vad de mindre gör. För de mindre organisationerna som har påbörjat att arbeta digitalt har dem då börjat med att digitalisera rekryteringsprocesser som ett första steg.

”Ja men jag tycker där är man ju bäst på det, både ute hos kunderna och också internt hos oss och jag undrar om det hänger ihop med att det har varit digitaliserat ett tag och att man kanske också där har det även innan GDPR tycker jag har funnits en medvetenhet om att man måste ha kontroll på dom dokumenten och den informationen.” – I:2, 2022

En fråga där svaren i empirin skiljer sig något åt är frågan gällande kompetens hos HR-avdelningarna att hantera digitaliseringen. Här svarar de intervjupersoner som arbetar ute i andra organisationer den generella kompetensen är ganska låg, men att det finns en ambition och medvetenhet i vad som behövs göras.

”Jag tycker att den generella kompetensen är ganska låg och jag tycker att intresset ganska lågt det finns en ambition, alltså på något sätt så finns det en förståelse för det, man är ju med på att det behöver göras men man har inte täckt det där gapet av att själv lära sig det som krävs så att det är, man skjuter det framför sig.” – I:2, 2022

”Nej, faktiskt upplever jag i två av de projekten jag jobbar med just nu, de organisationerna har implementerat HR-systemen, och så har de inte haft tillräcklig kompetens, så de har bara implementerat de IT konsulterna har sagt, det är så här man gör” – I:5, 2022

De intervjupersoner som arbetar på HR-avdelningar svarar att kompetensen finns men med tillägg av intervjuperson 3 att kompetensen finns för det man har beslutat att göra inom digitalisering i nuläget, men att det är en annan diskussion om det gäller något som avdelningen önskar göra.

”I den omfattning man gör, ja! vi har de som behövs för vad har vi bestämt att göra och det tror jag också dom flesta organisationer har det... Men om du tänker vad önskar man göra, det är en annan grej och vissa blandar ihop, jag önskar ha allt och att man kan gör allt med en knapp och så ja det kan man göra men det är inte det som vi investerar nu eller det vi har bestämt eller beslutat att göra.” – I:3, 2022

Intervjuperson 6 anser att det finns en bristande kompetens men att det också kan vara en rädsla hos organisationen att digitaliseringen kan komma att förändra processer i organisationen.

”Däremot så har vi ju inte, det kan vara en kombination då av bristande kompetens och viss mån rädsla också, därför att för att låta då digitaliseringen och de möjligheter som en digitalisering kan innebära att låta det påverka och förändra våra kärnprocesser i verksamheten, affärsprocesser och andra verksamhetsprocesser, där är vi inte speciellt bra. Dels beror det nog på att vi har

bristande kompetens men jag tror det också beror på att man känner sig lite att bekymrade för vad det här får för konsekvenser så det finns en viss rädsla.” - I:6 , 2022

Gemensamt för intervjupersonerna är att de alla ser att det finns utmaningar med att digitalisera HR. Intervjuperson 2 beskriver en utmaning i att förlita sig på tekniken, men bortse från att det även krävs tid att lära sig det nya systemet, nya arbetssätt och en ny inställning från organisationen.

”Jag ser en utmaning i att man förlitar sig lite för mycket på tekniken att hon inte förstår tillräckligt mycket att det kräver också att man måste förhålla sig till alltså arbetssätten och inställningen måste ändras. Man kommer också behöva jobba på mycket mer att för det kräver på något vis att alla vill lära sig nya saker ständigt om man ska digitalisera den takten som krävs med alla nya saker som kommer.” – I:2, 2022

Detta är något även intervjuperson 3 tar upp och beskriver dels utmaningen i att digitalisera i den takt som organisationen kan ta emot den, dels vikten av att organisationen ska förstå nyttan av digitaliseringen för att fullt kunna dra nytta av den.

”Det kan handla om folk som inte tycker om teknik och digitala verktyg, de kan hamna om deras ålders påverkande, det många olika orsaker. Så det är också den mest utmaning, den mest känsliga grejen med digitalisering. Så man behöver också vara försiktig med hur långt man går med digitalisering och anpassa det, för om man tänker HR, vi behöver ha det i takt med hur våra anställda kan ta emot och digitalisering ” – I:3, 2022

Intervjuperson 4 beskriver utmaningen i att få engagemang till förändring från organisationen.

”Utmaningen är alltid är att få engagemang, alltså förändringsledning, change management, att få folk att förstå varför dom ska ändra arbetssätt och då menar jag inte bara chefer medarbetare utan även alla inom HR. Det handlar också om att ofta så implementerar du system som stöd för processerna och då om det är stora företag med många lokala avknoppningar så måste man kanske se över och börja jobba mer likartat och det är en förändringsresa som kan heta duga i vissa fall för att det kan vara jättesvårt att få folk att ändra sitt sätt att se på sina processer.” – I:4, 2022

Även intervjuperson1 ser organisation och organisationens förmåga att integrera digitala tjänster med andra processer, som en utmaning med att digitalisera HR.

”Organisation, organisationens förmåga att ta till...och nu menar jag inte att vi inte kapabla, men generellt sett med digitalisering och inte bara kopplat till (organisationen), utrullning av nya tjänster och lösningar, och hur det tas emot hur integreras med andra processer. Det är den största utmaningen.” – I:1, 2022

4.4 Informationssäkerhet

Empirin visar sedan att intervjupersonerna och deras organisationer arbetar olika med informationssäkerhet. Både intervjuperson 1 och 4 beskriver hur deras organisationer jobbar med informationssäkerhet i stor utsträckning och systematiskt.

” Ja jättemycket, det finns ju otroligt mycket människor som jobbar med det... det här det är ju ett av våra absolut viktigaste områden med tanke på vår affär...” – I:4, 2022

”Systematiskt skulle jag vilja påstå, vi utgår, vi har ingen, vi certifiera inte oss mot någon ISO standard, det finns det absolut inget behov av för vår verksamhet men däremot är utgår vi från ISO standarder och vi specifikt egentligen går vi in från eller gå vi utgår vi från LIS, så lite systemet för informationssäkerhet som MSB har tagit fram och vi implementerar dom delar som går att implementera här och nu vi plockar liksom, så att man tar inte in hela systemet utan man plockar det som behövs. så utifrån det anpassar vi organisationen och skriver till på olika parametrar så det är ett systematiskt arbete.” – I:1, 2022

Intervjuperson 2 beskriver att informationssäkerhet är ett dilemma för dem som organisation i start-up fasen.

”...det är liksom startup bolagens dilemma liksom att sådana saker kommer ganska långt ner på listan, att man inte sätter rutiner tidigt, och det kan ju vara all form av informationssäkerhet, det som vi har på vår hemsida eller när vi skapar listor för personer eller våra egna anställda eller nej där har vi ett jobb att göra tycker jag.” – I:2, 2022

Intervjuperson 6 tar upp problematiken med informationssäkerhet att det ofta kolliderar med bekvämligheten och funktionaliteten i verksamheten och att det kan vara lättare att inte arbeta informationssäkert även om man är medveten om riskerna med det.

”problemet med informationssäkerhet det är att det kolliderar med bekvämlighet och funktionalitet... frestelserna att ta the easy way out, för det går mycket fortare än att då hantera det på en korrekt informationssäkerhet sett... man önskar ju att det fanns någon gordisk knut som man med ett alexanderhugg kunde öppna upp genom att köpa någon pryl men så är det ju inte utan informationssäkerhet är ju primärt, beteenden, processer, rutiner och policys. Så det är jobbigt att vara informationsäker, även för någon som vet vikten av det som jag.” – I:6, 2022

Fortsättningsvis tar intervjuperson 3 upp en annan aspekt av informationssäkerhet där det påverkar hela organisationen på en stor skala då det blandar olika avdelningar men också att det är en stor investering för en organisation i relation till de regler som finns uppsatta.

”det också känsligt, ganska komplicerat för många, för att det blandar legala och juridiska folk och det blandar verksamhet och operation och alla möjliga avdelningar i och det kostar mycket om man gör fel, det och det kostar också mycket om man vill göra rätt, för att så att behålla ett företag i linje med GDPR, i

linje med lokala lagar och samtidigt vara transparent och effektiv den här balansen med att vara transparent och compliant, är svårt. det kan man göra men man behöver lägga mycket tid och energi och pengar för att behålla den här balansen” – I:3, 2022

Alla de intervjupersoner som arbetar i HR-roller nämner att dem arbetar med informationssäkerhet i sina roller. För intervjuperson 2 och 5 har informationssäkerhet varit en aspekt som på ett eller annat sätt tagits upp i uppdrag som de i sina konsultroller fått genomföra.

”Vi varit inne på informationssäkerhet då när vi ska implementera ett HR system för att komma upp frågor om var lagras persondata någonstans och då finns det något fall där man har studerat om det om det kan lagras i USA eller i Europa och det finns liksom vissa regelverk då för hur persondata kan lagras” – I:2, 2022

”Det som jag hjälper mycket till är att säkra mig att när vi gör en HR-process är att vi också diskuterar de här rollerna som är involverade i processen. Det första är att man begränsar hur många som ska vara med i processen för det är ganska ofta så ser man att i verksamheten så finns det två eller tre eller fyra approvals på en process men det är ju folk som sätter kontroller och det gör att för det första sprider man data så det är ganska mycket folk som är med, och som har tillgång till data” – I:5, 2022

Intervjuperson 4 och 3 beskriver att informationssäkerhet är väl inarbetat i arbetsrollens rutiner och en del av de vardagliga arbetsuppgifterna.

”...det är ju de här basgrejerna som är superviktiga, vad får man göra, vad får man printa, vad får man mejla, var får man, hur får man hantera data, men det men det börjar ju sitta i nästan i ryggmärgen det är ju ingenting som man ens tänker på längre... självklart jobbar vi med det hela tiden men det är så inarbetat i rutinerna att du nästan inte ens tänker på det längre skulle jag säga i alla fall dom som jobbar så pass mycket i system som mitt team.” – I:4, 2022

”I min roll behöver jag hela tiden bli uppdaterat och följa dom här linjer, riktlinjer som finns, sen är det att ha koll genom många olika sätt, på löpande koll, man kan inte gå in i detaljer med varje user men man behöver ha en övergripande koll på hur är läget men hela tiden och uppdaterar eller ändrar, när det behövs, när det krävs, när man känner eller när det dyker upp nya behov.” – I:3, 2022

Att det finns en risk att obehöriga får tillgång till känsliga data i samband med att man digitaliserar stora delar av HR-processerna ser alla intervjupersoner. Intervjupersonerna har däremot lite olika insikter som de lyfter i samband med frågan. Intervjuperson 1 tar upp vikten av att ha ett moln och SaaS strategi som innefattar åtkomst och autentisering- och valideringsmetoder.

”Ja men det är klart det är allt det finns ju alltid man måste ha en molnstrategi man måste ha en SaaS strategi och det har vi i och det innefattar allt från åtkomst till autentiseringsmetoder validets metoder” – I:1, 2022

Intervjuperson 3 tar upp att det är en ständig medvetenhet om risken att obehöriga får tillgång till data:

”Det är en risk som det finns hela tiden och du kan förhindra hur mycket som helst men det kan inte göra risken noll... Det är en grej som man tänker på när man arbetar hela tiden, att inte göra det lättare för HR-data blir i obehöriga händer” – I:3, 2022

Vidare tar intervjuperson 6 upp att risken att obehöriga får tillgång till data fanns även innan digitaliseringen men att digitaliseringen i sig skapar fler ytor till att något sådant sker.

”det var det fanns det redan innan man digitaliserade och nu när vi digitaliserar då ökar vi ju bara riskexponeringen och vi skapar fler... så här, i vår bransch så pratar man ju om angreppssektorer och i och med att vi digitaliserar mer och mer så ökar vi ju liksom ytan, vår sårbara yta mot omvärlden, så att det är för vekt att bara säga ja, det gör det, utan det gör det exponentiellt, digitaliseringen ökar risken och utsattheten exponentiellt och det är ju obra kan jag ju säga.” – I:6, 2022

Intervjuperson 5 ger ett exempel på hur mycket personal-data hanteras på ett sätt som gör det lätt för obehöriga att få tillgång till data från en organisation som hen arbetat med.

”Jag har också sett i ett företag där jag jobbat med var de gör compensation planering i ett excel ark och där de sände ut excel-ark och så skriver folk tillbaka i excel-ark utan lösenord, och så ligger det compensation data för tusentals personer i emails, så det ser jag stadigt” – I:5, 2022

Även om det tas upp att det är viktigt att se till att obehöriga inte får tillgång till data, tar intervjuperson 2 upp vikten av att säkerställa att rätt personer också har tillgång till rätt data.

”... dels hur man kontrollerar, ja men som jag var inne på här olika behörigheter i system och hur säkerställer vi att vi hanterar det data som vi får tillgång till rätt och sen så är det leverantörer som skulle det ju fler olika parter och väldigt att många människor egentligen som skulle kunna få tillgång till känsliga data och hur säkerställer man då att man trycker på rätt knappar på något vis.” – I:2, 2022

Detta är något som intervjuperson 1 också beskriver:

”...i den upphandling vi gör nu till exempel vårt system där är väldigt mycket fokus på roll behörigheter och rollstyrning otroligt mycket.” – I:1, 2022

Intervjuperson 2, 3 och 6 tar avslutningsvis upp tre intressanta aspekter av informationsmationssäkerhet i samband med att det är HR-processer som digitaliseras och betonar hur den typen av data påverkar verksamheterna.

”man ska värna om individen tänker jag, alltså det blir ju så tydligt att man får mycket, mycket, mer information om personer i ett system än vad man haft tidigare och speciellt om man digitaliserar HR som man har ett system där man ja det kan vara mål och utvecklingsamtal, det är löneuppgifter, det är data om personen på ganska många nivåer då har du ju det på ställen på ett helt annat sätt än vad det kanske hade tidigare, det medför processer och rutiner och liksom jag tänker mig hela People Analytics delen med statistik och uppföljningar så här det kräver ju också ett ganska stort ansvar för att hantera det rätt.” - I:2, 2022

”HR som funktion är inte så olika än de andra. Vi har samma risker samma utmaningar som finans, som verksamhet och operation och andra delar med

informationssäkerhet och med digitaliseringsresan men det som gör HR annorlunda är att det påverkar våra anställda, så det är hela företaget, en organisation i sitt core är en del medarbetare tillsammans. Det är inte är datorer och bord och stolar, det är folk som arbetar tillsammans ett gemensamt mål och det påverkar dem direkt. det är kanske det som gör det annorlunda eller kanske mer känslig eller farligt på något sätt” - I:3, 2022

”det är just det är ju att vi för över mer och mer, både beroende och värde, i saker vi inte kan ta i, immateriella tillgångar och vi har inte hängt med när det gäller att skydda det här. Det finns ju så många enkla sätt att beskriva det, nu sitter vi hemma bägge två men, ta en människa på sin arbetsplats, om han eller hon kommer hem och någon har varit och stulit deras storbilds-TV då ser de det med en gång när de kommer hem för den är borta och den stod där i morse och stod inte där nu. Information kan du stjäla utan att någon har en aning om att det överhuvudtaget är på villovägar för den finns ju fortfarande kvar.” – I:6, 2022

4.5 Säkerhetsbrister vid digital HR

4.5.1 Tekniska hot

Vidare identifierar intervjupersonerna flera andra olika risker och hot som berör informationssäkerhet gällande digitalisering av HR. Flera av intervjupersonerna identifierar tekniska hot så som ransomware attacker och hackning.

”...utöver det så och det som fällorna om vi pratar om dem och då har det ju phishing då har ju ransomware det är väl det som tar väldigt mycket social engineering” – I:1, 2022

”Det är en risk som det finns hela tiden och du kan förhindra hur mycket som helst men det kan inte göra det noll. Man kan tänka på de stora, stora, stora frågor cyber attacker och så, risken finns, vi har ett dagligt arbete för att det inte händer och vi försöker att det blir mindre risk och att det inte händer, men risken finns och risken finns hos alla.”- I:3, 2022

Intervjuperson 5 beskriver även en bristande kunskap kring den typen av hot mot organisationer.

”där upplevde vi hacking, var några personer de fick tillgång till en profil på en medarbetare i (***) kontoret, genom hacking. Och så kommer de in i systemet. Och det är något, det var ett ganska stort företag så vi hade en bra process för att hantera det men hela frågan kring hacking, det är något som efter det, när jag kom hem till europa och kom hem till Danmark, där ingen talar om hacking, folk tror inte det finns till. Det är ett ting hur man beskyddar sin data men ett annat ting är hacking, hur man upptäcker hacking, the stains från hacking, för det händer också. Det är ett område som man inte har så mycket kännedom till eller bevittnat så.” – I:5, 2022

Vidare har GDPR haft en påverkan på samtliga intervjupersoners arbete i någon omfattning och de alla ger konkreta exempel på hur inträdet av direktivet påverkat hur organisationerna arbetar med informationssäkerhet.

”i mitt förra jobb som globalt ansvarig för HR-operation då var det en ganska stor del, så jag jobbade tätt in på vanlig HR, HR-policy department, med IT och med legal, om att göra ett helt framework, som vi hade, ett globalt framework för att säkra oss att hela organisationen globalt blev GDPR compliant”- I:5, 2022

”I varje del, behöver man ställa samma fråga, behöver vi all den här informationen ja eller nej, behöver jag spara den här informationen ja eller nej, behöver jag dela den här informationen ja eller nej, hur länge behöver jag spara det och vem ska ha access till och vad händer när det inte behövs och hur man raderar och hur ofta. De här frågor, gäller varje värde i våra HR-data, så det påverkar alla processer, alla rapporter, all datalagring, det är också en mentalitet förändring för oss och för dem som vi jobbar med.” – I:3, 2022

”ja jag tycker framför allt att det var det där med mailandet som påverkades mest att man blev så vars att just det får inte mejla sådana här listor hur som helst som gjordes liksom korsande och tvärsan mejlade alla möjliga känsliga uppgifter och också det här med att lagra data blev också en liksom det var ju jätte, jättestor skillnad. Det hade vi nog överhuvudtaget inte tänkt på tidigare, alla sparade sina personliga mappar och olika listor på personer och känsliga uppgifter så där” – I:2, 2022

Intervjuperson 4 nämner att det tagit tid för leverantörerna av systemen att även dem anpassa sina produkter efter GDPR.

”sen är det ju också i vissa fall kanske det tagit lite tid, att det släpat efter med tekniken ibland, att dom här större leverantörerna då måste ju uppdatera så att det går att följa lagarna och det har dom ju gjort men då har liksom dom varit... När, dels vi vet inte riktigt vad som krävs, vi vet inte riktigt vad leverantörerna kommer tillhandahålla för möjligheter, vi vet inte vad vi har för interna krav, så ja alltså allting rörde sig runt.” -I:4, 2022

Slutligen nämner intervjuperson 6 att GDPR ökat medvetenheten kring värdet av data och ger ett exempel på hur data utnyttjats i andra sammanhang

”...att medvetenheten om att information har på något sätt ett värde har ju ökat väldigt mycket, även om det i första hand inom GDPR är för att man är rädd för att få sanktioner mot sig. Jag tycker GDPR är bra, för när man vet vad man kan göra med personuppgifter och den digitaliseringen som vi trots allt har idag vad den innebär, då är det väldigt bra att man försöker sätta stopp på det här på något sätt. Det är bara se Cambridge Analytica hur man med all sannolikhet, ganska omfattande, påverkan det valet både i USA och brexit valet i England” – I:6, 2022

På frågan kring molntjänster har intervjupersonerna olika uppfattningar kring dess inverkan på organisationernas informationssäkerhet. Intervjuperson 2 och 3 tar båda upp upphandlingen av tjänsterna och möjligheten att ställa krav på dem.

”jag tycker att man noga ska gå igenom den delen av avtalet och undersöka hur, alltså hur säkerställer de att data inte hamnar i fel händer och ofta så har man ju olika produktionsmiljö, och testmiljö, hur säkerställer man att den rätt rensas med

jämna mellanrum och alltså så här lite städrutiner, personer som slutar hur får vi bort dom och också så här olika behörigheter i systemet tänker jag så att det inte är fel personer då som jobbar i det får tillgång till fel data.” – I:2, 2022

” vår systemleverantör som vi ställer krav på dem och vi väljer hela tiden dom som kan och de som har bra vision i informationssäkerhet och också dom har en del, för du vet nu att de flesta system i världen är moln, så helt enkelt att du har inte något i ditt företag alltså du har här en länk och en inloggning och så det är faktiskt hela data finns hos en leverantör så det är också när våra inköp och legal avdelning, så man behöver ställa rätt krav på leverantörer som man signar med och det tror jag vi gör det bra.” – I:3, 2022

Intervjuperson 4 tar också upp vikten av rätt leverantör av tjänsterna men menar även att den nivån av säkerhet som de stora leverantörerna av molntjänster kan erbjuda är något om de själva aldrig skulle kunna göra själva med de resurser de har.

”den säkerhet som finns kring de här stora leverantörerna av molntjänster, dom säkerhetsspärar som finns kring vår data skulle vi aldrig kunna göra själva, aldrig, vi har inte de resurserna. Här pratar vi ju liksom, det finns ju ett par stora leverantörer och dom hanterar ju data för otroligt många företag, har hela avdelningar som inte gör annat än att se till att data är säker därför att det är hela deras business handlar om det. Jag tror inte att vi någonsin skulle kunna ha varit i närheten av den säkerheten själva så att jag är inte ett dugg orolig men det finns fortfarande absolut oro och man ska vara man ska naturligtvis tänka till och vara försiktig och man måste se till att man har rätt leverantörer och att man har rätt typer av avtal och sådana saker men går man med någon av de här riktigt stora leverantörerna”- I:4, 2022

4.5.2 *Mänskliga hot och mänsklig faktor*

Den mänskliga faktorn, och misstag som begås av medarbetare ses också av flera intervjupersoner som en risk i arbetet med informationssäkerhet.

”den största risken är ju den mänskliga faktorn så är det alltså, det den största risken informationssäkerhet är den goda viljan brukar jag säga. Det kan vara den mänskliga faktorn är inkluderat och skickar fel mejl till exempel så att du sätter saker i cc och inte bcc om det är en hemlig kopia, det råkade skicka till fel person, med det händer ju.” - I:1, 2022

”men det är ett pågående arbete, det är också att utbilda folk, att väcka idéer eller att väcka konceptet hos folk att du inte behöver öppna varje länk du får och du behöver inte dela information via mejl utan du kan dela inne i systemet. Det är också en lärande resa, att sluta ladda ner och koppla ert mejl och skicka och jag är för allt som är fel adress det skickades till en annan person, det är därför vi har ett system där man kan dela information där inne. det är också mycket åtgärder och information som man behöver uppdatera dom som använder alla verktyg.” – I:3, 2022

Intervjuperson 6 tar upp sina egna erfarenheter kring den mänskliga faktorn och HR funktionens roll i det.

”HR har eller alltså personalfunktionen och en enormt viktig del i informationssäkerhet, inte som teknikbärare utan liksom som kulturbärare. Jag har jobbat väldigt mycket mot både militära och polisiära underrättelser och säkerhetstjänster, då har de ju ändå mäktiga fiender men alla landar i samma definition och det är att över tiden så är insidern alltid det största hotet alltså det är liksom personalen, som medvetet eller omedvetet, gör så att man får informationsförluster, så det visar ju på behovet att både kontrollera sina medarbetare och utbilda dem.” – I:6, 2022

För att förebygga risker arbetar flera av organisationerna med att utbilda sina medarbetare inom informationssäkerhet, några mer generellt och andra mer riktat mot den enskildes roll i verksamheten.

”Alla medarbetare måste gå flera utbildningar som handlar om informationssäkerhet årligen så att det är obligatoriska utbildningar både som nyanställd och sen måste den uppdateras minst en gång per år och det är inte bara en utan det är flera olika.” - I:4, 2022

”... man behöver anpassa den här informationen utskick eller kurs till hur mycket den här personen behöver verkligen. För att en person som är som jobbar i verksamheten, har inget managementansvar, inget HR ansvar, inget finansansvar, han har jättelåg tillgång till information så behöver inte veta mycket om det. Så hög du har tillgång till information, du behöver veta mer och du behöver bli mer medveten.” – I:3, 2022

”Vi har återkommande utbildningar, jag satte upp awareness-utbildningar som går en gång per månad och som följs upp och dom är automatiserade, jag får statistik på dom och så kan jag alltid peta på och justera till näst kommande utbildningar utifrån resultatet för föregående utbildning. Så det är det ena, dom tar ju 3 minuter att göra så det är 3 minuter utbildningar. Sen har vi en punktinsatser till exempel vid varje onboarding så får varje nyanställd är ett frågebatteri eller utbildningsmaterial heter det men några kontrollfrågor och så vidare, det för att ge insikt i hur vi arbetar med informationssäkerhet så att det är en del av onboarding processen och sen ibland så blir det ju punktinsatser där det känns att det behövs, till exempel nu är det väldigt ransomware attacker vi behöver fräscha upp det då har vi utbildningspaket som vi skickar ut och så får som vi ja får svar på.” – I:1, 2022

4.5.3 Informationssäkerhetsincidenter

Skulle det ske informationssäkerhetsincident i våra intervjupersoners organisationer, har de olika rutiner för hur de hantera det. Beroende på vilken roll intervjupersonerna har i sina verksamheter har de olika insikter i hur arbetet kring informationssäkerhetsincidenter går till.

”Vår process att vi har ju incidentteam med en incident manager och jag är med där från början, jag är med i teamet, så att en incident manager sköter projektet när det gäller incidenten och jag är den som hanterar frågorna och gör bedömningar i frågorna om GDPR är det bland annat i det här men även informationssäkerhet över lag. Till mitt förfogande har jag ett dataskyddsombud och han är direkt externt sådant och honom har jag koll med, har jag god kommunikation med heter det, så att incidenten kommer, vi hantera det, vi identifierar, vi tappar till

eventuella ifall det skulle behövas att något håll eller om de någon risk eller minska riskerna och åtgärddar därefter utifrån olika processer vi har ju olika processer och olika nivåer på incidenter så då hanterar vi det eftersom det.” – I:1, 2022

”om det skulle hända, det ska, jag vet inte ja, det här inte hänt så jag vet jag kan inte berätta exakt hur det kommer och fungera. Men om något händer, är det en kris som företaget ska hantera genom deras krishantering policy och GDPR-policy och datasäkerhetspolicy. Jag tror att de finns hos IT och där dom ska ta fjäder för att fortsätta nya arbeten med incidenter.” – I:3, 2022

”Beror alldeles på hur allvarligt det är. Vi skriver alltid en rapport och den skickas till chef som sedan avgör om den ska skickas vidare till datasäkerheten eller IT-säkerhet beroende på alldeles beroende på. Men vi skriver alltid en incidentrapport på oavsett vad det är men och väldigt ofta är det så pass begränsat och smått så att det inte blir någon stor grej av det men det händer ju att det skickas vidare då och då finns det finns ju processer och rutiner för det” – I:4, 2022

”Vi har faktiskt på min telefon och min computer där har vi att det står när jag startar min computer så står numret på får IT-desk om man har security incident, så jag har blivit tränad i vår security policy så om man upplever något som har hänt så känner jag till processen till det nummer jag ska ringa. Så antingen sender jag ett email eller ringer till ett nummer men där har vi support 24/7 på det om det sker någon incident. Så vi känner till de stegen vi ska rapportera om det här.” – I:5, 2022

5 Diskussion

I detta avsnitt analyseras studiens insamlade empiri mot den teori som presenterats i litteraturgenomgången. Syftet med detta avsnitt är att identifiera samband och presentera eventuella likheter och skillnader mellan tidigare forskning och intervjupersonernas upplevelser. Därefter kommer de utmaningar och lärdomar som identifierats diskuteras med mål att identifiera vilka informationssäkerhetsutmaningar som uppkommer i samband med att man digitaliserar HR-processer och hur dessa utmaningar hanteras.

5.1 Digitalisering

I avseende digitalisering visar litteraturstudien att det kan bidra till en ökad produktivitet och standardisering i organisationerna. Vidare innebär digitalisering inte bara ett teknikbyte utan också ett förändrat arbetssätt (Börjesson, 2020). Detta är något som flera av intervjupersonerna också betonar, bland annat intervjuperson 1 som beskriver hur digitaliseringen kommit att inkluderas i organisationen verksamhetsstrategi och hur digitaliseringen har bidragit till att de nu kan erbjuda sina tjänster både fysiskt och digitalt (I:1, 2022). Detta är också något som intervjuperson 3 beskriver, att det är ett pågående projekt i att digitalisera och att de ständigt ser över sina processer (I:3, 2022).

Även arbetsplatserna påverkas av digitalisering och att medarbetare kommunicerar alltmer genom digitala hjälpmedel. Det förändrar också hur medarbetare förhåller sig till varandra och till organisationen. (SOU 2016:85, Jesuthasan, 2017). Detta är något som kan avspeglas i hur digitaliseringen mottas i organisationerna. Empirin visar att det är en blandad reaktion bland medarbetarna. Intervjuperson 5 beskriver mottagandet från organisationerna som optimistiskt och lite naivt, där många ser det som att IT-system löser allt men inte förstår att implementeringen i vissa fall kan innebära mer arbete. Flera av de andra tar upp vikten av att skapa en förståelse för förändringen och att digitaliseringen då mottas bättre (I:4, 2022). Även en ledning som är drivande i frågan kring att digitalisera ses som något som bidrar till en positiv attityd mot digitaliseringen (I:1, I:3, 2022)

5.2 Human Resources i kontext av digitalisering

I litteraturstudien beskrivs begreppet Digital HR som något har utvecklats i syfte att generera en värdefull informationsdatabas över de mänskliga resurserna i en organisation. Dessa olika verktyg skapar tillsammans ett övergripande HR-system, ett e-HRM, där de olika verktygen kan integrera med varandra (Stone et al., 2015). Nästan samtliga intervjupersoner beskriver i empirin att dessa verktyg används i deras verksamheter. Vidare beskrivs det i litteraturstudien hur man kan ta vara på den stora mängden data som genereras genom att digitalisera HR vilket i sin tur gör användningen av artificiell intelligens möjligt (Trost, 2020). Ingen av intervjupersonerna i studien nämner självmant att de använder artificiell intelligens på den nivån i sina organisationer. Det är något som verkar ligga längre fram i digitaliseringsprocesserna.

Något annat som framkommer i litteraturstudien av Panayotopoulou et al. (2007) är att utbildning av personalen är en avgörande faktor för att implementeringen och användningen av digitala HR-system ska vara lyckat. Detta kan speglas i empirin där flera intervjupersoner beskriver att den generella kompetensen kring digitalisering bland HR-avdelningar är låg, tillräcklig för det man gör men inte för det man vill göra men att ambitionerna oftast finns där (I:2, I:3, 2022). En av intervjupersonerna beskriver ett scenario där två olika organisationer implementerat nya system enligt externa IT-konsulter men har själva inte kompetens nog att utnyttja och driva dessa system efter implementeringen (I:5, 2022). Det beskrivs också organisationer som förlitar sig på tekniken och bortser från att det krävs tid att lära sig det nya systemet, nya arbetssätt och en ny inställning (I:2,2022). Vilket är i enlighet med Panayotopoulou et al. (2007), som hänvisar till förståelse och utbildning som en avgörande faktor för en lyckad digitaliseringsprocess.

Gemensamt för alla intervjupersoner i empirin när att de ser utmaningar i att digitalisera HR. Utmaningen i att digitalisera i den takt som organisationen kan ta emot den, dels vikten av att organisationen ska förstå nyttan av digitaliseringen för att fullt kunna dra nytta av den är en av utmaningarna som tas upp (I:2, 2022). En annan är utmaningen att få engagemang till förändringen, och skapa en förståelse för varför de ska förändra sitt arbetssätt (I:4, 2022). Detta är något som också kan härledas till litteraturstudien och de avgörande faktorerna om lyckad implementering som presenteras av Panayotopoulou et al. (2007).

5.3 Informationssäkerhet

Grunden till god informationssäkerhet anses enligt Stallings & Brown (2018) vara de tre komponenterna confidentiality, integrity och availability (Stallings & Brown, 2018). Enligt litteraturstudien uppvisas god konfidentialitet genom att skydda obehörigas åtkomst till data, dels genom att förhindra att informationen når fel personer, dels att se till att rätt personer faktiskt gör det (Möller, 2020). Utifrån intervjuvaran som presenteras i empirin upplever alla intervjupersoner att det finns en risk i samband med att stora delar av HR-processerna digitaliseras att obehöriga får tillgång till känsliga data. Uppfattningen hos en av intervjupersonerna är emellertid att risken även fanns innan man digitaliserade men att i och med att man digitaliserar har riskexponeringen ökat (I:6, 2022). Det framkommer likaså att i många av organisationerna finns det en medvetenhet kring riskexponeringen och att man arbetar proaktivt för att minska den risken (I:3, 2022). Ett sätt som organisationerna arbetar med det är genom att ha en strategi som innefattar åtkomst och autentiserings- och validesmetoder kommer upp i empirin (I:1, 2022)

Fortsättningsvis beskriver litteraturstudien integritet som den andra viktiga komponenten till god informationssäkerhet. Det innebär att den data som lagras i systemen är korrekt, tillförlitlig och inte ändras av personer som inte ska kunna ändra den (Wyllder, 2003). Detta är något som verkar vara en större utmaning enligt empirin. I en av intervjuerna tas ett exempel upp från en organisation som skickade olåsta Excel-ark med kompensationsdata för tusentals personer emellan sig (I:5, 2022), något som gör det lätt att dels obehöriga får tillgång till data, dels att data ändras. Vidare beskriver en av de andra intervjupersonerna ett dilemma kring stöld och ändring av immateriella tillgångar där du kan stjäla eller ändra dessa utan att ägaren har någon vetskap om att det har hänt för informationen fortfarande finns kvar (I:6, 2022).

Avslutningsvis är den sista av de tre komponenterna, tillgänglighet. Den syftar till att information, data och program ska vara tillgängligt och aktuell för behöriga användare när det

behövs (Möller, 2020). Många av intervjupersonerna beskriver detta som något som får utrymme i diskussioner och förarbeten ute i organisationerna. I exempelvis upphandling av nya system så är rollbehörighet och rollstyrning en del som avhandlas (I:1, I:3, I:5, 2022).

Informationssäkerhet syftar till att skydda informationstillgångar med hjälp av policys, utbildning, träning, medvetenhet och teknologi (Whitman & Mattord, 2011). Empirin tyder på att flera av de organisationer som intervjupersonerna arbetar i eller med använder sig av policys och utbildningsinsatser för att skydda sina informationstillgångar. Dessutom beskrivs rutiner kring informationssäkerhet vara en del av det vardagliga arbetet för några av intervjupersonerna.

Däremot framställer empirin också två dilemman som uppstår för organisationer i samband med informationssäkerhet. För det första tar en av intervjupersonerna upp att informationssäkerhet hamnar långt ner på "att göra listan" för start-upp bolagen då det är andra uppgifter som behöver prioriteras (I:2, 2022). Detta kan stödjas av några av de andra intervjupersonerna som beskriver att informationssäkerhet ofta kolliderar med bekvämligheten och funktionaliteten i verksamheten samt att det är en kostnad för en verksamhet att vara informationssäkra, både när man gör fel och för att se till att organisationen gör rätt och är i linje med de lagar och direktiv som är uppsatta (I:3, I:6, 2022).

5.4 Säkerhetsbrister vid digital HR

En av de stora säkerhetsriskerna med HR-system som presenteras i litteraturstudien är de tekniska hoten som finns (Lillkrona, 2022). Cyberattacker som görs av hackare för att stjäla data, infektera datorer eller ta kontroll över datorer, system och nätverk. Några av de cyberattacker som presenteras i litteraturstudien är virus, ransomware, scareware, trojaner och så vidare (Evans et al., 2021). Likaså identifieras tekniska hot i empirin som en risk med digitalisering av HR. Hot som ransomware attacker och hacking nämns av flera intervjupersoner (I:1, I:3, 2022). Vidare nämns det att det är ett dagligt arbete att minska risken för den typen av hot (I:3, 2022). Även bristen på kunskap och medvetenhet bland HR-avdelningar tas upp som en risk av en av intervjupersonerna som upplever att det inte är många som har den vetskapen i att förstå och hantera sådana hot (I:5, 2022).

GDPR, den allmänna dataskyddsförordningen som infördes 2018 ställer höga krav på hur organisationer behandlar sina anställdas personuppgifter men även kunders och blivande medarbetares (Lillkrona, 2022). Från empirin kan man tyda att GDPR har haft en stor påverkan för samtliga intervjupersoner i hur de arbetar med informationssäkerhet både genom framtagandet av nya ramverk, policys och i de vardagliga arbetsuppgifterna (I:2, I:3, I:5, 2022), och skapat en medvetenhet kring värdet av den data som organisationerna har (I:6, 2022). Däremot finns det en uppfattning att systemleverantörerna tagit tid att anpassa systemen efter den nya lagstiftningen och att det därför inte alltid varit helt lätt att snabbt kunna anpassa organisationens arbete (I:4, 2022).

Litteraturstudien tar upp molntjänster som en möjlig riskfaktor för informationssäkerhet i samband med att HR-processer digitaliseras. Det finns en diskurs i hur säkra molntjänster faktiskt är (Popović & Hocenski, 2010). Även i empirin delas åsikterna kring molntjänster och hur de påverkar organisationerna. Ett flertal av intervjupersonerna påpekar att är viktigt att ställa krav på leverantörerna vid upphandling av molntjänster för att säkerställa att de fyller de

krav som organisationerna har på säkerheten (I:2, I:3, 2022). Ett annan aspekt som kommer upp i empirin är att molntjänsterna kan leverera en annan säkerhet än organisationerna själva kan göra med de resurser som de har och att de därför är ett bra alternativ (I:4, 2022).

En av de främsta anledningarna till säkerhetsbrister och incidenter är människor och den mänskliga faktorn (Skrodelis, Strebko & Romanovs, 2020). Detta är något som flera av intervjupersonerna också hävdar i empirin. Den mänskliga faktorn och risken att en medarbetare gör något omedvetet eller medvetet som riskerar organisationens informationssäkerhet anses av fler av intervjupersonerna vara den största risken (I:1, I:3, I:6, 2022).

Fortsättningsvis tyder empirin på att utbilda sin personal, väcka konceptet och idéerna kring hur man ska arbeta informationssäkerhet är något som inte helt tar bort risken för mänskliga fel men minskar dessa (I:3, 2022). Detta kan ta stöd i litteraturstudien där Siponen (2000) anger att skapa medvetenhet bland anställda genom utbildning som en av de främsta åtgärderna för att minska antal misstag som sker på grund av den mänskliga faktorn (Siponen, 2000).

6 Slutsats

Det huvudsakliga syftet med denna studie var att undersöka vilka informationssäkerhetsutmaningar som uppstår i samband med att HR-processer digitaliseras samt hur dessa hanteras av organisationerna. Den forskningsfråga som skulle besvaras löd:

”Vilka utmaningar relaterade till informationssäkerhet kan uppstå i samband med digitalisering av HR-processer och hur kan dessa hanteras?”

Studien har visat att digitaliseringen och digitaliseringen av HR-processer i synnerhet medför sina egna utmaningar för HR-avdelningarna. Digitalisering är inte bara ett teknikbyte utan också ett förändrat arbetssätt som måste etableras i organisationerna. Digitaliseringen bemöts olika ute i organisationerna och de påverkar också hur mottaglig verksamheten är för förändringen. I nuläget har flera av verksamheterna i denna studie etablerat digitala system, några arbetar med dem som en självklar del av arbetsvardagen andra är i en uppstartsfas men de möter fortfarande samma utmaningar i att digitalisera i takt med organisationens utveckling och att kompetensen inte alltid finns för att göra allt det man önskar göra, men däremot är tillräcklig i många fall för vad man gör i nuläget.

Vidare kan studien konstatera att medvetenheten kring utmaningar och risker med informationssäkerhet i samband med att HR-processerna, finns där. Många är medvetna om de risker som finns, mänskliga och tekniska och arbetar aktivt med policys, utbildning och medvetenhet. Andra verksamheter har inte kommit lika långt i arbetet kring att hantera dem och att förebygga dem men där har studien kunnat identifiera andra utmaningar.

Organisationer i start-upp fasen har inte alltid informationssäkerhet högst upp på att göra listan, för andra kolliderar säkerhetsfrågorna ofta med verksamhetens bekvämlighet och funktionalitet och dessutom kan det vara kostsamt för alla typer av verksamheter, både att arbeta helt informationssäkert, och att inte göra det alls. Något som studien däremot kan tydligt visa på är att införandet av GDPR 2018 gjorde det tydligt för många verksamheter vilket värde den data de förvaltar har, och vilka risker som finns om den data hamnar fel. För många organisationer ledde GDPR till flera förändringar i sättet att arbeta med informationssäkerhet.

Avslutningsvis är det som en av intervjupersonerna nämnde i sin intervju kanske egentligen inte så stor skillnad när det kommer till digitalisering och informationssäkerhetsrisker och utmaningar som i andra funktioner i organisationerna. Det är samma risker och utmaningar när det kommer till tekniska hot så som malware och ransomware attacker, den mänskliga faktorn och obehörigas tillgång till data. Men den stora skillnaden är att det påverkar organisationernas anställda, dem som gör företaget, kärnan av verksamheten, på ett helt annat sätt och det är det som gör det mer känsligt för en organisation. Det är en stor investering för en organisation att digitalisera och digitalisera i enlighet med informationssäkerheten, men när det handlar om en av de mest värdefulla tillgångarna, medarbetarna, bör det endast ses som en god investering.

6.1 Förslag till fortsatt forskning

Genom denna studie har det konstaterats att det finns flera utmaningar gällande informationssäkerhet i samband med att HR-processer digitaliseras i allt större utsträckning.

Denna undersökning har utgått från ett bredare perspektiv som undersökt flera olika aspekter, därför hade det varit intressant att fokusera på enbart en av utmaningarna som framkommit och gå vidare in på djupet av denna. Det hade även varit intressant att höra perspektiven från personer som arbetar med informationssäkerhets samt HR i samma organisationer, för att vidare kunna jämföra upplevelser samt se till skillnader i hur informationssäkerhet och digitalisering upplevs i samma organisation.

7 Bilagor

Bilaga A - Transkribering Intervju 1

Vilken är din roll på företaget och vilket arbetsområde är du verksam inom?

Absolut, jag är informationssäkerhetsansvarig. Kort och gott handlar det om att säkerhetsställa att all form av information som vi hanterar har rätt typ av tillgänglighet, rätt typ av skydd, rätt typ av riktighet kan man kalla det för, att data är korrekt, att den är säker och tillgänglig på korrekt sätt genom korrekta kanaler.

Skulle du kortfattat kunna beskriva ert företag?

Jag jobbar för en stiftelse som jobbar med omställningen av tjänstemän bland annat.

Vilken bransch tillhör ni?

Oj, det är en kombination, det är en omställningsbranch, det är väl HR, utbildning, stiftelsen är en kombination av försäkringskassa, arbetsförmedling, utbildningsverksamhet, omställningsorganisation, en kombination, så HR antar jag är det närmaste

1) Digitalisering

Hur arbetar ni med digitalisering på din arbetsplats?

Digitalisering är egentligen en del av DNAt. Lång historia kort... med en bakgrund, förut, med förut så menar jag 4-5 år sedan, så var inte digitaliseringen inte en del av organisationens dna men sen fick vi en nyhet till chef som satte det som en digital strategi, som är parallell med alla andra strategier bara för att liksom komma in i second phase, en andra andning, och sen blev den digitala strategin är en del av vår huvudstrategi, verksamhetsstrategi helt enkelt.

Så digitaliseringen är a och o, den är primär, det innebär att rent konkret att alla tjänster som vi idag erbjuder fysisk eller har erbjudit fysiskt ska kunna erbjudas digitalt och det primära utvecklingsområdet egentligen är att vi utvecklar våra tjänster och funktioner så allt ska kunna vara tillgängligt digitalt.

Hur har digitalisering påverkat din roll och dina arbetsuppgifter?

Otroligt mycket, det blir otroligt mycket mer för att helt plötsligt måste du tänka i flera dimensioner. Det blev fler lager av tillgänglighet. Om du sitter på ett fysiskt möte, då kan du och jag prata om... självklart finns det en säkerhet däremellan att vi sitter i rum med 4 väggar helt plötsligt flyttas det ut, till zoom eller teams.

Men utöver det så kanske finns dokument och dokumentation runtomkring. Det blev många aspekter på det på det hela, inte minst ur ett juridiskt perspektiv där vissa lagar spelar in och sätter krav på hur till exempel ett möte ska föras, var det är för information som får flöda, var data får lagras och hur det tillgängliggörs och så vidare. Så det har påverkat att det har blivit mycket mycket mer, man får... man får trippa på på varje gång man köper in en lösning eller tjänster man ska utveckla någonting.

Vilka utmaningar ser du med digitaliseringen?

Organisation, organisationens förmåga att ta till...och nu menar jag inte att vi inte kapabla, men generellt sett med digitalisering och inte bara kopplat till (organisationen), utrullning av nya tjänster och lösningar, och hur det tas emot hur integreras med andra processer. Det är den största utmaningen.

Vad innebär begreppet digital HR för dig?

Automatiserade processer tänker jag på.

Vad använder du för digitala HR-verktyg på din arbetsplats?

Vi är just nu mitt i en upphandling av ett nytt HR-system som ska automatisera HR-processer ännu mer. Vi har ju HR system, alltså HRM system, klassiska liksom vilken personal vi har, delar av onboarding processen, det funkar kanske inte så bra idag kanske men det är därför vi byter ut det. Vi har ju ekonomisystem, lönehantering

och så vidare så att det är en hel del digitala system, gruppförsäkringar, kommunikationen med leverantörer. Digitala kommunikationsverktyg, hela Microsoft 365.

Skulle du säga att er HR-avdelning har tillräcklig kompetens inom området för att hantera digitaliseringen?

Absolut, det tycker jag.

Har din HR-avdelning fått någon utbildning inom området?

Det är mycket kulturellt arbete att införa, att säga införa digitaliseringen låter så gammalt, men förstå mig rätt liksom digitalisering är ett kultur arbete och det är med acceptans nivån liksom organisationen... man jobbar brett, man jobbar inte med isolerade... liksom att du som person är... som avdelning ska kunna ta emot någonting eller vi använder liksom en annan typ av metodologi där vi jobbar med hela organisationen och kulturen för att acceptera förändringar och jag tycker att vi på (organisation) är exceptionellt duktiga på att ta emot nya lösningar.

Hur mottas digitaliseringen av er organisation?

Popcorn effekten, känner du till den? Ja det är lite så, det finns alltid några som poppar först av alla i mikron liksom och sen finns alltid sådana som blir nästintill utbrända mot slutet. Det är lite samma princip, alla behöver olika tid på sig, så det tas emot väl, och det hela handlar om att paketera värde, alltså nyttorealiserings liksom, varför gör vi det här, vare sig det handlar om inköp av nytt system att säkra upp nya processer, varför gör vi det. Jag tror när du paketerar det bra och jobbar med kulturen och acceptansen då tas det emot på mycket, mycket, bättre sätt än att du ska bara slänga ut system och säger till någon "nu ska du använda det här" för det funkar sällan bra. Så jag tycker att det tas emot väldigt bra, för att vi har vi har bra process för implementation.

2) Informationssäkerhet

Hur arbetar ni med informationssäkerhet på din arbetsplats?

Systematiskt skulle jag vilja påstå, vi certifierar inte oss mot någon ISO standard, det finns det absolut inget behov av för vår verksamhet men däremot är utgående vi från ISO standarder och vi specifikt, egentligen, utgår vi från LIS, ledningssystem för informationssäkerhet, som MSB har tagit fram och vi implementerar dom delar som går att implementera här och nu vi plockar liksom. Så att man... tar inte in hela systemet utan man plockar det som behövs. Så utifrån det anpassar vi organisationen och skriver till på olika parametrar...så det är ett systematiskt arbete.

Har ni en informationssäkerhetspolicy eller en informationssäkerhetsstrategi?

Ja det har vi

Hur ser arbetet ut för att etablera den?

Man bryter ner den i små beståndsdelar. Vi har en informationssäkerhetspolicy och den i sin tur har... man gör en analys av det. Varje gång du inför någon ny policy så genomför man en analys liksom, en konsekvensanalys och den hade en stor påverkan på digitala utvecklingen och då arbetar vi fram nya rutiner specifika för den digitala utvecklingen kopplat till denna, det vill säga att man konkretiserar informationssäkerhetspolicyen för den digitala utvecklingen. Hur påverkas vi? alltså ända ner till utvecklingsteamet, hur genererar vi fejk-personnummer? hur gör vi så här? hur arbetar vi med rensning? privacy by design, privacy by default, hela den biten liksom, så du konkretiserar det... Så att absolut, det påverkar andra delar också. Vårt kontaktcenter, hur påverkar det dom, liksom att ta emot... ja men då vi har en säkerhetspolicy som utgår från att man ska validera alla inkomna begäran från våra klienter som det heter, då måste vi upphandla ny telefoni som har mobilt bankID autentiseringen till exempel och det måste sättas in i en process, så har vi jobbat.

Hur arbetar man med att få ut informationssäkerhetspolicyen i andra delar av organisationen där man kanske inte aktivt arbetar med den varje dag?

Deltagande, alltså operativt deltagande i verksamhetens alla utvecklingar... alla avdelningar. Så jag är exempel den som är med i alla utvecklingsmöten, nej inte alla utvecklingsmöten men många utvecklings möten, de här nyckelmötena liksom, synkroniserings mötena är jag med avdelningsmöten, där jag pratar om informationssäkerhet. Där jag petar och hela tiden går in och liksom påminner liksom... att det här behövs skrivas till och då oftast kopplat till vad vi har för gällande regelverk. Sen använder jag mig väldigt mycket av mina fantastiska kollegor, som är chefer, liksom så det är genom dem, de blir mina satelliter lite grann och olika ansvariga, vi har ju produktansvariga, och då kan man gå igenom dom och säga att det är viktigt att era produktägare känner till dom här dom här koncepten och här gäller att vara liksom lite någorlunda smart och man kan inte slänga på ett sätt ett stort dokument på någon utan det handlar om att bryta ner det, för att du måste

du måste konkretisera det som är relevant, till exempel om vi pratar om någon utveckling av en viss funktion då behöver du adressera säkerhets perspektivet kopplat till dokumentet. Då kan säga vi behöver göra A för att vi har beslutat om Y i det här och det finns ju mer att läsa av där. Så det är man måste vara väldigt operativ.

Hur arbetar ni med att utbilda personal inom informationssäkerhet?

Vi har återkommande utbildningar, jag satte upp awareness-utbildningar som går en gång per månad och som följs upp och dom är automatiserade, jag får statistik på dom och så kan jag alltid peta på och justera till näst kommande utbildningar utifrån resultatet för föregående utbildning. Så det är det ena, dom tar ju 3 minuter att göra så det är 3 minuter utbildningar. Sen har vi en punktinsatser till exempel vid varje onboarding så får varje nyanställd är ett frågebatteri eller utbildningsmaterial heter det men några kontrollfrågor och så vidare, det för att ge insikt i hur vi arbetar med informationssäkerhet så att det är en del av onboarding processen och sen ibland så blir det ju punktinsatser där det känns att det behövs, till exempel nu är det väldigt ransomware attacker vi behöver fräscha upp det då har vi utbildningspaket som vi skickar ut och så får som vi ja får svar på.

Vilka är de stora informationssäkerhetshoten som ni upplever?

Det beror på om du med säger hot så är det en grej, säger du risker en annan grej, låt mig ta båda. Alltså den största risken är ju den mänskliga faktorn så är det alltså, det den största risken informationssäkerhet är den goda viljan brukar jag säga. Det kan vara den mänskliga faktorn är inkluderat och skickar fel mejl till exempel så att du sätter saker i cc och inte bcc om det är en hemlig kopia, det råkade skicka till fel person, med det händer ju. En annan grej den goda viljan, det vill säga att någon ringer in, vi är så otroligt serviceminded på (organisation), och så kanske någon ringer in och säger, och gråtande och säger jag behöver ändra mitt bankkontonummer jag har ekonomisk kris, jag behöver få ut mina pengar och så vidare så här och då kanske du känner du att du är en jättegod människa och vill hjälpa till så absolut lugn jag hjälper dig. Det ska ju akta oss för och det gör vi inte och därför har vi visa processer tidigt för att validera personer. så att den människan absolut största risken sen har vi liksom utöver det så och det som fällorna om vi pratar om dem och då har det ju phishing då har ju ransomware det är väl det som tar väldigt mycket social engineering, det är väl dom tre.

Har ni fått någon specifik utbildning i hur ni ska arbeta med informationssäkerhet just i din roll?

Ja ja jag har gått en ska vi se vad kallades den utbildningen, informations säkerhetsstrategi, det för det är 5 olika kurser som sitter ihop som man blir diplomerad i efteråt.

Vilka utmaningar ser du med hur ni arbetar med digitalisering kopplat till informationssäkerhet?

Hänger med! Alltså saken är att beroendena, vi har ju otroligt många tjänster och funktioner och det gäller att hålla tungan rätt i mun, för du har ju dels verksamhetsbehovet, dels har du de juridiska kraven och dels har de tekniska förutsättningarna. Så en utmaning med informationssäkerhet är att du få ihop allting, för att när du utvecklar en ny funktion då ska du tänka vilka beroenden har den till andra funktioner och konsekvenser har den. Då behöver kanske sätta dit en någon form av funktion, det kan vara autentiseringen, det kan vara data restriktioner eller vad kan vara för någonting. så skulle vilja påstå, förutom det sagt jag sagt innan med organisationen att få den och acceptera dom här den här nödvändiga funktioner som du lägger på så tycker jag att hålla koll på allting, alltså informationssäkerhet i sig anser jag, subjektiv åsikt, inte är en komplex, det är inte en svår fråga så, det är bara komplexiteten ligger i mängden för frågor som du bollade, behöver ha hålla i luften och digitaliseringen går ju väldigt fort framåt, kraven på organisationen de ökar ju på olika håll och leveransförmåga måste ju öka och då måste informationssäkerhet att hänga med för att en ny funktion kan tillgängliggöra data från annat ställe och då måste du hänga med ska man applicera samma typ av regelverk överallt samma typ av nivå överallt så är väl det som är utmaningen att hänga med på allting.

Hur påverkade införandet av GDPR lagstiftningen ert arbete?

Oj, varje dag, varje fråga, GDPR den finns där hela tiden

Har ni behövt förändra sättet att arbeta eller organisationen på något sätt på grund av GDPR?

Absolut vi har förändrat sätt att arbeta, vi har förändrat den tekniska arkitekturen infrastrukturen, copy, UX, allt har ändrats utifrån GDPR

Upplever ni att det finns en risk eller utmaning med att obehöriga får tillgång till känsliga data i samband med att man digitaliserar stora delar av HR-processerna?

Ja men det är klart det är allt det finns ju alltid man måste ha en molnstrategi man måste ha en SaaS strategi och det har vi i och det innefattar allt från åtkomst till autentiseringsmetod validets metoder och så vidare så där känner mig ganska trygg. För vi har ju en stark upphandlings grupp, inköps grupp, där jag bland annat ingår så att det finns ingenting smått eller stort som köps in till organisationen utan att det går igenom oss och då pratar vi drift, arkitektur, informationssäkerhet och så vidare så där har jag känner ingen risk alls men det är klart eller

känner ingen oro alls men det är klart risken finns ju alltid för du är i händerna på en leverantör och du och då du kan ju validera deras processer via papper alltså de har ju deras styrdokument men faktum är att det är fortfarande människor som jobbar där de kan göra fel och då är det viktigt att ha processer och rutiner fastställda från början till exempel hur gör ni vid en incident, hur får vi reda på informationen, hur ABC. Så de frågorna är väldigt viktiga vid upphandlingen och genom dem kan man känna sig mer eller mindre trygg då med upphandlingen och jag tycker att vi är väldigt duktiga på det.

Inom organisationen så att jag inte är orolig, för att i den upphandling vi gör nu till exempel vårt system där är väldigt mycket fokus på roll behörigheter och rollstyrning otroligt mycket. Upphandlingen tar en bråkdel av tiden det är egentligen implementation som tar stora delen testning och implementation, synkronisering, så ur vårt perspektiv är inte orolig det är klart det finns risker ja det finns det men jag är inte orolig för vår del och uppstår det något problem på grund av mänsklig faktor för det vi människor som testat dom här säkerhetsreglerna så har vi ju förmågan att processa att det som åtgärder.

Om det sker en informationssäkerhetsincident i er organisation, hur arbetar ni för att hantera det?

Vår process är att vi har ett incidentteam med en incident manager och jag är med där från början, jag är med i teamet, så att en incident manager sköter projektet när det gäller incidenten och jag är den som hanterar frågorna och gör bedömningar i frågorna om GDPR, är det bland annat i det här men även informationssäkerhet över lag. Till mitt förfogande har jag ett dataskyddsombud och han är direkt externt sådant och honom har jag koll med, har jag god kommunikation med heter det, så att incidenten kommer, vi hanterar det, vi identifierar, vi täpper till eventuella ifall det skulle behövas att något hål eller om de någon risk eller minska riskerna och åtgärdar därefter utifrån olika processer vi har ju olika processer och olika nivåer på incidenter så då hanterar vi det eftersom det.

Är det någonting nu när jag har intervjuat dig som jag inte frågat dig om som du hade tyckt det hade varit en relevant att ta upp kring området?

Du berörde det, den ena frågan, och det är ju det är med organisation och utbildning att göra. och jag vet inte om det är inte så att du inte berör det men jag tror man ska en fråga som är väldigt viktig är ju återigen den enskilda individens förmåga och dels acceptera den funktionen som det innebär och lägger på olika säkerhetsrutiner, dels förstå och implementera den egna vardagen. Det är absolut, det är en viktig parameter som jag har haft man ska ha olika KPIer liksom för att mäta liksom hur om jag gör ett arbete med informationssäkerheten men jag lägger en till en utbildning eller förändrar någonting hur mäter jag så det är det väl den frågan, hur mäter du förändringar i organisationen ur ett informationssäkerhetsperspektiv. Det vill säga att era insatser ger bang for the bucks, ni får valuta för pengarna. Det är en fråga som du kanske kan lyfta upp liksom för det är en viktig punkt i informationsarbete det är uppföljningsarbetet för att det är nog i uppföljningsarbetet som du kan identifiera brister. En annan grej som är mer av teknisk karaktär, hur jobbar ni med hur arbetet ifrån säkerhet handlar om situationen och då finns olika tekniska aspekter på det hela men vilka verktyg använder ni vilka digitala verkliga användning för att säkerställa att ni har en god säkerhetsnivå.

Hur jobbar ni med att mäta informationssäkerhet? Återkopplingen?

Olika sätt, är det men för mig är den primära utgång från utbildningsperspektivet det vill säga oppositionen som många att förstå det jag säger eller ha en ökad nyfikenhet eller visat intresse för det och det är mängden ställda frågor till mig. I och med att jag är den som får svara på de frågorna helt enkelt det finns ingen annan, det ena, mängden antalet frågor som ställs angående GDPR och angående informationssäkerhet.

Det andra, den djupare parameter, är mängden avancerade frågor och då kan det vara så att någon har det innebär då tänker mig vad är en avancerad fråga det kan vara så enkel fråga är ju så här, får vi skriva får vi spara den här informationen om den här personen är en enkel fråga, en avancerad fråga kan vara så här okej men vi har förstått att vi ska säga till alla att vi ska spela in ett sånt här möte via zoom, men hur gör vi om en person accepterar men visade sig senare vara på grund av grupptryck. 12 personer sitter ett möte 11 säger ja men självklart kan du spela in, den äldste vill inte vara här party poopern, den vill inte vara den personen, hur gör vi då? och den är ju lite intressant för att den har man inte ett svar på i första hand utan då måste man prata om det eller liksom med dataskyddsombudet med chefsjuristen och så vidare och behöver vi sätta rutiner har det hänt innan eller så här det är lite kittlande frågor så vi mäter liksom antalet frågor, enkla frågor generellt och sen de avancerade frågorna och dom är inte så vanligt förekommande liksom det är ändå intressant så det är ett perspektiv. det andra är ju olika copyer egentligen kopplat till digital utveckling, ja som olika utvecklingsteam ens frågor kopplat till digital utveckling.

Säkerhetsmekanismer, lösningar?

Jag har satt upp en mindmap egentligen som delar upp informationssäkerhet ur ett, du har ju ett budget perspektiv och du har affärsperspektiv, du har HR, compliance, legal, revision och så och en av dem är

Operation of Security ska säga, och där går man in på olika sätt, det har ju liksom penetrationstester är det ena till exempel, att du kan automatisera penetrationstester, du kan arbeta med code Reviews, vilket vi gör också, det har använt med architecture by code, och de ena och det andra, så man inte bygger hela din molnstruktur, hela din applikation utgår från olika typ av kontroller det har ju automatiska mjukvaror som kontrollerar koden du skriver och sen testas din kod och samtidigt så har du olika unit tests, och du har ju team testing och det har acceptans testning innan det går till kanske stageing miljö där man testar i verksamhetsperspektiv innan man går vidare och så du har olika nivåer och du pratar bara digital utveckling.

Sen har de olika det har ju liksom nätverks övervakning, du har ju funktions övervakning av AB(?) övervakning, du har olika liksom övervakningar som skickar varningssignaler ifall något till exempel är nere, det här är någonting som är konstigt. En annan grej som vi jobbar med just nu med upphandlade är ju beteendeanalys i nätverk exempelvis, hur gör vi för att identifiera diverse beteenden, ännu en grej är regional access vad får man nå data från vilket land eller och så vidare, identity management controller, brandväggar, entity protection som man pratar om väldigt mycket så väldigt mycket säkerhet och det är säkerhet är ju inte ett program utan det är ju liksom väldigt mycket mer om man pratar ett tekniskt perspektiv men till syvende och sist är säkerhet lika med människa för du kan ju köpa 50 70 olika programvaror mjukvaror och tjänster men det räcker med att en person trycker på fel knapp så kan man stänga av allt det där och någon kommer in.

Arbetar ni med informationssäkerhet redan i rekryteringsprocessen av anställda?

alltså det ena är ju det är väl på vilken typ av verksamhet vi har inte den verksamheten att vi gör en bakgrundskontroll till exempel brottsregister och sådant där vi har inte den verksamheten. men däremot det som är högst relevant för oss är ju det som var inne på tidigare det är prio- och onboarding det vill säga att man du får ta del av hur vi arbetar med informationssäkerhet och att du får tillgång till alla all vår dokumentation.

Vi har ju till exempel ett intranät insidan där vi samlar väldigt vi samla allting för att det är pedagogiskt, så den behöver man få tillgång till på ett på ett bra sätt. det är också en viktig grej att ta med och ha i baktanke för den som jobbar med informationssäkerhet det är att det inte ska skapas hyll dokument liksom utan du när du skapar någonting så ska det ska stå på ren svenska om man får säga så och om man har ett dokument är väldigt betungande då måste man ju någonstans tillgängliggöra informationen på ett lättsmält sätt liksom, så det jobbar vi med också och den som ansvarar för de dokumenten måste ha en kommunikativ någorlunda kommunikativ förmåga för att och vara pedagogiskt för att utbilda. Så att egentligen är i rekryteringen så nämner vi givetvis, så har vi liksom en del att GDPR och den personliga integriteten är väldigt viktig för oss men det är inte förrän man skrev på avtalet som man får dom här utbildningarna då skickade till sig som man kan i förväg liksom eller under jag tror ändå onboarding just nu är det osäkert om det är pre eller onboarding som man får utbildningen att gå igenom.

Hur många anställda är ni och hur många är ni som arbetar med informationssäkerhet?

Konsulter och fulltime över 350 kanske, jag är inte så säker där ish runt där med konsulterna tror jag och antal personer som jobbar med informationssäkerhet det är en person, det är jag som är ansvarig.

Har du något team eller så som du kan bolla med?

ja gud, väldigt mycket IT givetvis men jag tillhör inte IT alltså rent organisatoriskt tillhör jag ju HR och det är en annorlunda placering ofta är man antingen ett eget team, egen avdelning eller så tillhör man IT faktiskt men jag tycker det är fel att tillhöra IT för med HR är du objektiv och du behandlar alla lika snällt och lika hårt. och du ska vara verksamhetsövergripande jag tror att den tjänsten kan finnas också om man är ensam person som jag är så kan det finnas inom någon form av verksamhets- och utvecklingsavdelning för det är det där man kan ligga också. men det är en person och är inget specifikt team som jobbar med informationssäkerhet men däremot har jag mitt team av nyckelpersoner låt oss kalla det för det, kanske är lite vanskligt uttryck, alla är lika viktiga, men det finns ju vissa personer jag har liksom driftchef, chefsarkitekter, incident manager, du har IT-chefen, sen har du chefsjuristen och så här som personer som jag alltid bollar med och datorskyddsombudet givetvis som är väldigt mina go to guys liksom, inköpsansvarig och så vidare.

Etik, hur jobbar ni med etiska frågor kopplat till informationssäkerhet?

Det är en väldigt viktig fråga för att vi samlar data i enlighet med överenskommelser, samtycken, avtal och sådant där och då ska vi ju använda den informationen enbart för det syftet. Vi använder aldrig informationen, det står också uttryckligen vår informationssäkerhetspolicy, så finns ett etiskt stycke om det, om att data aldrig får användas för annat syfte än vad det är menat för och i den omfattning är mer att till och inom den tidsramen därefter ska allting raderas och så vidare. Så att du kan exempelvis inte samla namn och postnummer som kan du liksom kombinera ihop, triangulära dem på något sätt, för att skapa liksom en tredje data. Det kan du göra om

det för samma syfte till exempel att vi hjälper folk i omställning och det utvecklar ny tjänst men vi kan aldrig använda det för att liksom utveckla nya tjänster.

Till exempel och det är också en sådan utmaning i GDPR och informationssäkerhet om jag får följ svara på tidigare fråga, det är just det här att du måste ju ta hänsyn till dom avtal, det måste hela tiden följa dom avtalen som ni har tecknat och det är era i ett eget regelverk och det kan ibland sätta käppar i hjulet för viljan och skapa fler funktioner. för då måste du återigen införskaffa ett nytt samtycke eller uppdatera samtycke eller intresseanmälan det finns en skillnad mellan de 2. och den gör att det blir folk säger men den här funktionen är otroligt bra för klienten den skulle verkligen vilja hjälpa dig men jag förstår jag accepterar men vi måste införskaffa ett samtycke.

Det kan vara så enkelt som att vill du delta i är att testa våra nya funktioner, vill vara en testperson eller vill du, det tillhör inte syftet omställning, så då måste vi ska införskaffa denna intresseanmälan från personer och då får vi ju då måste vi göra på ett säkert sätt så kopplat till etik så skickar vi mejl till alla våra klienter som enbart handlar om vill du vara med är utan då får det vara till exempel, då får det bakas in i ett generellt mejl som vi har. Så om de har signat upp sig och då kan det vara ett stycke i mejlet, förresten vi genomfört dessa tester vill du vara med eller i samtal med rådgivare så det är etiska perspektivet kopplas in där också så att det inte känns som att man vi håller på att sälja in saker vi vill utveckla nya funktioner som kom in kom in liksom utan det ska alltid kännas bekvämt för den som har information hos, klienter, kunder och över det.

Bilaga B - Transkribering Intervju 2

Vilken är din roll på företaget och vilket arbetsområde är du verksam inom?

Jag har ju en blandad roll så att det är både vd för (organisation) och jag är senior HR Tech konsult ute på företag och jag är också konsultchef då för mina anställda så att jag är hjälper dem i deras uppdrag.

Skulle du kortfattat kunna beskriva ert företag?

Vi är en koncern som jobbar inom HR, vi jobbar både med search rekrytering och med people Consulting som det heter, HR konsulter som är ute på företag och ersätter ofta en roll som HR chef eller HR business partner eller går in för att förstärka HR grupper eller utvecklare så där och sen så HR Tech vi är specialiserade på digitalisering av HR och det vi gör då det är att vi dels så kan vi gå in och göra förstudier hos företag som funderar på att digitalisera HR funktionen på något sätt och då gör vi egentligen en kartläggning av nuläge så vi gör intervjuer med nyckelpersoner i organisationen och kollar på, frågar efter hur upplever dom HR leveransen och vad är det dom saknar för att det skulle kunna bli effektivare och smartare och sen så håller vi också i workshops där vi där vi också sätter ett önskat läge alltså om man då tittar gör en gap analys egentligen och titta på om ni är här nu vad siktar ni mot och vad ser ni framför er när det fungerar som bäst och vad är det som behöver hända då och då är det bara det vad som behöver hända i deras förändrade arbetssätt men också vad är det för verktyg och digitala hjälpmedel som skulle förändra deras arbetssätt.

Sen så är vi också inne och jobbar som projektledare när företag väl har valt en lösning så kommer vi in och driver alltså projektleder det projektet alltså är kundens mottagare och har kontakt med leverantören så att man köper in låt säga Workday så hjälper vi ju till att svara på alla frågor som leverantören har eller varit en spindeln i nätet och ledare från kundens sida och sen avslutningsvis så kan vi också komma in som stödresurs när företag har nåt slags HR system på plats för att förbättra och utveckla det som är uppsatt så ett sånt uppdrag är jag inne på nu till exempel där jag ja då har dom ett HR system sen 2 år tillbaka men det funkar inte som dom hade tänkt så då måste vi skruva på processerna och göra om lite och förbättra och förfina.

Vilken bransch tillhör ni?

Ja just det var är det fördelningen brukar vara, alltså vi är ju konsulter vad kallar man det och tjänster var, tjänstebranschen.

Hur många anställda är ni i er organisation?

Totalen så är vi runt 20 och i HR Tech så är vi just nu 6 anställda

1) Digitalisering

Hur arbetar ni med digitalisering på din arbetsplats?

Det var ju en bra fråga det gör vi ju nästan inte alls skulle jag säga så vi lever inte som vi lär vi är väldigt så där Excel baserade idag vi har ett rekryteringssystem, vi har till exempel inget säljsystem som vi kanske skulle behöva ha, vi har inte heller något system för konsulter och man skulle ju kunna tänka sig något verktyg där man har alla konsultprofiler och så där så att det vi har är egentligen rekryteringssystem, vi har ett system som heter fortnox där man gör alla löner och där man fakturerar och så där alltså ett redovisningssystem men thats it, och LinkedIn då förstås och de alltså eller ja Instagram och Facebook är väl det vi jobbar med men i övrigt så är vi inte så digitaliserade tyvärr.

Hur har digitalisering påverkat din roll och dina arbetsuppgifter?

Det där är svårt nu när jag liksom är dubbla roller så ska jag tänka då utifrån min chefsroll där jag är anställd eller ska jag tänka liksom i uppdrag tycker du?

Ta båda perspektiven det kan bli intressant.

Ja nej men digitalisering är ju liksom våran affär där jag jobbar det är det som ger oss nya uppdrag det är det mina konsulter lever på nåt vis och vårt företag det är ju att vi ser ett stort behov av att företag behöver digitalisera så att det är det som gör att vi har existensberättigande på något vis att vi ser ett jättemånga behöver digitalisera men dom vet inte riktigt hur man gör alltså dom har inte den kompetensen själva och det är där vi kommer in och hjälper till så att det har ju påverkat oss jättemycket och kommer också göra det jättemycket det känns som att det är precis starten.

Vilka utmaningar ser du med digitaliseringen?

Jag ser en utmaning i att man förlitar sig lite för mycket på tekniken att hon inte förstår tillräckligt mycket att det kräver också att man måste förhålla sig till alltså arbetssätten och inställningen måste ändras. Man kommer också behöva jobba på mycket mer att för det kräver på något vis att alla vill lära sig nya saker ständigt om man

ska digitalisera den takten som krävs med alla nya saker som kommer. Så behöver man också arbetsteam som är villiga att lära sig nya saker och där tycker jag att det haltar och speciellt HR måste vara mycket mer framåtlutade om vi vill digitalisera HR då måste vi gå i bräschen för det på företagen det är ingen annan som kommer visa hur det ska vara utan HR funktionen måste själva vara väldigt uppdaterade på vad som händer och där ser jag jättestora utmaningar, dom vill ofta inte alls.

Vad innebär begreppet digital HR för dig?

Ja jag tänker att digital HR, då tänker jag att det är dels att det är vissa processer som är automatiserade som man inte längre gör som man gjorde tidigare. Jag tänker också att det finns en annan nivå där man kanske digitaliserar genom att flytta vissa arbetsuppgifter till ett annat verktyg så att det inte blir automatiserat men man jobbar i andra verktyg för att utföra det, tänker jag, och sen så tänker jag också digitalisering av HR handlar om att få ihop att hitta Work Tech balans så att man också jobbat man sätter ihop de olika verktygen i strömmar som flödar väldigt fint och utan alltså helst ska ju slutanvändaren inte ens märka att man rör sig mellan olika system, det hade ju varit liksom målet på något vis. Visionen.

Om du tänker din roll som konsult, hur upplever du den generella kompetensen inom digitalisering på de HR-avdelningar du besöker

Jag tycker att den generella kompetensen är ganska låg och jag tycker att intresset ganska lågt det finns en ambition alltså på något sätt så finns det en förståelse för det man är ju med på att det behöver göras men man har inte täckt det där gapet av att själv lära sig det som krävs så att det är, man skjuter det framför sig.

Får HR-avdelningarna någon utbildning hur de ska arbeta vidare med digitaliseringen i samband med att ni hjälper dem?

Nej, känslan är ju att jag tycker HR generellt sett har väldigt väldigt mycket att göra man har byggt upp sin funktion så att det man får någon slags existensberättigande eller man finns till för att man hela tiden har väldigt mycket att göra och då jobbar man reaktivt som man jobbar på förfrågan från verksamheten och då är man inne i någon slags snurra av att ständigt ha jätte jätte jätte mycket att göra och då med det så finns det ganska lite tid över att jobba proaktivt och tänka framåt så hade man liksom avsatt tid vilket jag tror alla funktioner behöver göra man behöver avsätta tid för att lära sig nya saker och gjorde man det så skulle man också man skulle vinna tid på sikt det är det som är ironiska i hela men man tar sig inte den tiden när man utan man är i den här ekorrhjulet på något vis väldigt

Hur mottas digitaliseringen i organisationerna ni arbetar i?

Ja jag tycker att det som händer ofta när man antingen som väljer man enkla tools, eller appar eller verktyg där det ger ganska snabb effekt som till exempel så finns det ju en referens app som man kan använda för referenstagning den är väl går väldigt snabbt och implementera kan komma i gång på några veckor och då blir det ju så här en wow känsla verkligen att Gud vad bra det här blev. samma sak dom som väljer att gå över från pappersdokument till e-signatur till exempel det är också en sådan här wow vad bra det blev. men om man gör lite större delar som ett HR-system till exempel där blir det till en början så blir lite sämre alltså då upplevs det första året tror jag många upplever att det här blev ju mycket sämre än vad vi hade det tidigare så att det tar mycket längre tid innan det ger den effekten som man vill ha och så tror jag det känns i dom lägena.

Skulle du säga att det mottas olika om det är en ung eller äldre organisation?

Jag tycker så här unga människor som kommer ut i arbetslivet dom har ju generellt sett mycket högre krav på digitalisering de förväntar sig att vad ska jag så här kan det väl inte gå, alltså dom har mycket högre nivå än vad dom tycker är lägsta nivån på hur det ska funka och speciellt där tror jag att det gör avtryck i onboardingen att man som nyanställd bara vad är det frågan om ska jag sitta här och läsa den här luntan 50 sidor papper om hur det funkar. Där tycker jag att det man ser tydligt att det är så att det är liksom skillnad mellan generationer vad man är van vid. Men sen apropå din fråga så ser jag också en stor det är inte säkert att ett företag som ligger i framkant som har ett erbjudande i sig där själva kärnan är väldigt digitalt det är inte säkert att HR är Digitalt för det nej det finns ju liksom ingen logik i att det ska spegla varandra.

2) Informationssäkerhet

Hur arbetar ni med informationssäkerhet på din arbetsplats?

det är vi ju inte så bra på, vi har verkligen ett jobb att göra där och jag vet inte om det är liksom startup bolagens dilemma liksom att sådana saker kommer ganska långt ner på listan, att man inte sätter rutiner tidigt, och det kan ju vara all form av informationssäkerhet, det som vi har på vår hemsida eller när vi skapar listor för personer eller våra egna anställda eller nej där har vi ett jobb att göra tycker jag.

Har ni några säkerhetsrutiner?

Ja nej alltså det är ju hemskt att svara på det men nej det tycker inte som skulle liksom hålla om vi blev granskade.

Hur arbetar ni med att skapa medvetenhet kring informationssäkerhet på din arbetsplats?

Jag tror att det är många av oss har med oss för att vi har jobbat på andra bolag tidigare det är ju att man kanske undviker att skapa alltför detaljerade listor till exempel som man vet att man inte får göra om det inte fyller något syfte eller funktion och också att man kanske tänker på att slänga dom där Excel-arken eller vad det nu är efter ett tag att man inte sparar massa massa dokument som man inte har någon nytta av så tänker jag i alla fall att det här känns inte GDPR mässigt och samma sak som när vi kallade till ett event häromdagen så sparar vi inte sådana listor heller och vi var också noga med och att man klickar i då att den som anmäler sig att dom vet att dom hamnade i på en lista och så där så att i det lilla försöker vi göra det vi kan och att det finns en sån medvetenhet. Inom rekrytering, där vi har rekryteringssystem där är mycket lättare att jobba så då finns det inbyggt rensnings funktion och där samtycke att man ska fyller i att man hamnar i Ponty och så där så att där är det är ju mycket lättare när man har ett system.

Arbetar ni något med informationssäkerhet när ni är ute och arbetar som konsulter?

Nej än så länge har vi inte haft det inom vårt uppdrag, det har ju dykt upp lite kring den här vad heter den här fallet Schrems 2, det handlar ju om att data inte får alltså i ja jag kan den inte heller utantill men i alla fall så har vi varit inne på informationssäkerhet då när vi ska implementera ett HR system för att kommit upp frågor om var lagras persondata någonstans och då finns det något fall där man har studerat om det om det kan lagras i USA eller i Europa och det finns liksom vissa regelverk då för hur persondata kan lagras. Så där har vi varit delaktiga i det men vi tar inte ansvar för det nej.

Får ni samarbeta med de som är ansvariga för informationssäkerheten ute på företagen?

ja så till exempel om det är dags att implementera ett HR-system då vi tar det som exempel, då ser vi till att ha funktioner som tittar på det. Att man GDPR säkrar eller information säkrar dom systemen som vi tar in då måste det vara en del av avtalet att dom redogör för hur kommer data att hanteras och hur säkerställer vi att det här lagras på rätt sätt och vad finns det för rensnings funktion och vad har dom rättighet till och vad har vi rättighet till och så där så att det är ju en ganska naturlig del i så här molnbaserade system tycker jag

Ser du någon liksom risk i att laga så mycket persondata på ett moln eller ser du några utmaningar med det?

Ja alltså om man ser det ja alltså jag tänker att man ska absolut ta del av hur det uppsatt hos dom leverantörerna man väljer, alltså jag tycker att man noga ska gå igenom den delen av avtalet och undersöka hur, alltså hur säkerställer de att data inte hamnar i fel händer och ofta så har man ju olika produktionsmiljö, och testmiljö, hur säkerställer man att den rätt rensas med jämna mellanrum och alltså så här lite städrutiner, personer som slutar hur får vi bort dom och också så här olika behörigheter i systemet tänker jag så att det inte är fel personer då som jobbar i det får tillgång till fel data och så där så att jag tycker att man ska verkligen alltså så här dom stora systemen dom har ju helt klart sett till att dom är liksom fria i ansvar att dom har rutiner som dom kan hålla för dom har så otroligt många kunder och stora företag som dom samarbetar med som också har väldigt höga krav så på något sätt tänker jag att det känns säkrare där men jag tycker ändå inte man ska ta det för givet.

Är ni inblandade i upphandlingar av systemen ni hjälper till att implementera?

Då gör vi då hjälper vi kunder att göra kravspecifikationer om dom ska då skicka ut förfrågningsunderlag till leverantörer och då är det ett helt avsnitt med informationssäkerhet. Så man ställer då ett antal frågor kring deras informationssäkerhet, hur lagras data hur ser rensnings funktionerna ut också så här även vilka personer hos den här leverantören har tillgång till vårt data vilka kan se och göra saker med vår datainformation och hur säkerställer man att de har då rätt kompetens för att göra det och hur vet vi att dom är betrodda.

Har ni en informationssäkerhetspolicy eller en informationssäkerhetsstrategi?

Ja, nej och vi borde verkligen ha det men vi har inte.

Hur arbetar ni med att följa upp era anställdas kunskaper inom informationssäkerhet?

Nej.

Vilka utmaningar ser du med hur ni arbetar med digitalisering kopplat till informationssäkerhet?

Ja men jag tror att det här är liksom bara början på något den där här kommer bli absolut utmaningar alltså, dels hur man kontrollerar, ja men som jag var inne på här olika behörigheter i system och hur säkerställer vi att vi hanterar det data som vi får tillgång till rätt och sen så är det leverantörer som skulle det ju fler olika parter och

väldigt att många människor egentligen som skulle kunna få tillgång till känslig data och hur säkerställer man då att man trycker på rätt knapp på något vis.

Jag tror också utrensning alltså hur man städar data i en ganska stor del alltså att det inte ligger där en stor stor massa av information som man inte ska ha tillgång till längre, personer som har slutat för flera, flera år sedan och så där och det jag tror att det är så pass nytt med dom här systemen så att man inte har haft data så länge att man ser till att rensa i historiken.

nej men jag ser massa sådana utmaningar verkligen och jag tänker i Sverige är det ändå så att vi inte frågar så mycket jag tänker ju också när vi jobbar i globala projekt så blir det ju ännu tydligare det här vi har ju ändå inte alltför mycket data om personer. men i andra länder så frågar man ju jättemycket om man kan ju fråga liksom om etnicitet och militärtjänst gör öring och alltså massa information som jag tänker så här vad och då ska ju vi följa Sveriges lagar om vi lagrar dom i vår databas i Sverige och hur går det där ihop liksom det är den tänker jag regelverket kring det intressant om det är olika rättigheter i olika länder.

Hur påverkade införandet av GDPR-lagstiftningen ert arbete?

jag minns att, jag då hade ju lite annorlunda roll då 2018, men jag minns att det var jättestort det där och att det skapade väldigt mycket oro och att skillnaden mot för hur man hade jobbat tidigare, då hette det ju PUL personuppgiftslagen och att skillnaden till GDPR var ganska markant alltså att man blir väldigt medveten om att det sträckte sig över ett ganska stort område att det hade liksom med hur man mejlade och göra och bilder på personer och ja så där jag tyckte det var ganska stor grej när det kom.

Har ni behövt förändra sättet att arbeta eller organisationen på något sätt på grund av GDPR?

ja jag tycker framför allt att det var det där med mailandet som påverkades mest att man blev så vars att just det får inte mejla sådana här listor hur som helst som gjordes liksom korsande och tvärsan mejlade alla möjliga känsliga uppgifter och också det här med att lagra data blev också en liksom det var ju jätte, jättestor skillnad. Det hade vi nog överhuvudtaget inte tänkt på tidigare, alla sparade sina personliga mappar och olika listor på personer och känsliga uppgifter så där så att det nej jag tyckte det var stor skillnad och man blev väl också ganska skrämmd av att för då när det kom så minns jag att man tog in personen som skulle lära upp så man hade ju som olika insatser då för att lära personal om GDPR och då så blev man ju också varse att okej om jag gör fel så kan det bli ganska höga viten som straff. Sen vet jag inte om det har blivit så men det var så man sa då i alla fall.

Jag tror att man kanske skulle behöva göra lite granskningar att det är det som krävs vad skulle nog gå att behöva gå på något stort företag som har möjlighet att betala höga viten och så får det bli lite skrämselfekten.

Vilka är det största informationssäkerhets hoten eller informationssäkerhets riskerna med att man digitaliserar HR?

Ja nej men det är ju att man ska värna om individen tänker jag, alltså det blir ju så tydligt att man får mycket, mycket, mer information om personer i ett system än vad man haft tidigare och speciellt om man digitaliserar HR som man har ett system där man ja det kan vara mål och utvecklingssamtal, det är löneuppgifter, det är data om personen på ganska många nivåer då har du ju det på ställen på ett helt annat sätt än vad det kanske hade tidigare, det medför processer och rutiner och liksom jag tänker mig hela People Analytics delen med statistik och uppföljningar så här det kräver ju också ett ganska stort ansvar för att hantera det rätt ja.

Upplever du att folk har den kompetensen att kunna hantera det som är med och digitalisering?

Nej det upplever jag faktiskt inte, jag tycker inte det finns så stor medvetenhet om det som man skulle behöva ha. Nej och jag tänker alltså nej, jag tänker att det är ganska många funktioner i organisationer som har tillgång till väldigt mycket data, för att dom har det jobb, dom jobben. Till exempel om man jobbar som systemförvaltare eller så här på ett företag dom personerna har ju ofta admin rättigheter för att kunna göra justeringar och med det så känner dom ju också till väldigt och kan ju titta på allt möjligt liksom och där tänker jag att man kanske borde göra en insats och verkligen förklara det jag vet inte jag skriva sekretessavtal eller någonting för att medvetandegöra det mer.

Arbetar ni något med informationssäkerhet redan i rekryteringsprocessen?

Ja men jag tycker där är man ju bäst på det, både ute hos kunderna och också internt hos oss och jag undrar om det hänger ihop med att det har varit digitaliserat ett tag och att man kanske också där har det även innan GDPR tycker jag har funnits en medvetenhet om att man måste ha kontroll på dom dokumenten och den informationen. Alltså att man måste det vet att det var ju länge så här vi pratade om att man måste kunna gå tillbaka och titta på vem fick det här jobbet och utifrån diskriminerings perspektiv och så där så tycker jag att man har varit ganska noga där med att dokumentera och ha koll på det och där är det också tydligt att man också man vet nu att man

måste ha personers samtycke för att lagra informationen och att man därmed också måste söka via ett system för att vara aktuell för jobbet det tycker jag liksom har satt sig ganska bra jämförelsevis.

Om det sker en informationssäkerhetsincident i er organisation, hur arbetar ni med att hantera det?

Vi är så pass små så skulle det komma liksom någon och granska oss på något vis då tror jag verkligen att vi skulle skärpa till det och kanske liksom se över ska vi laga det här på något annat sätt. Men vi har också pratat om sådana här lösningar som att i våra i Microsoft att man ska ha en sån här tvåstegs identifiering vad heter det autentisering, säkra så att inte andra kommer åt våra data så att det har vi redan nu på gång men jag tror också att vi i och med att vi växer och nu är uppe i 20 konsulter så kommer vi behöva ha det här på ett annat ställe och då kommer också säkerheten komma med det men jag tror nu skulle vi om nån kom och granskade oss precis idag då skulle vi nog känna oss ganska så skakiga, då skulle vi då behöva göra en rejäl insats alltså hos alla oss som jobbar.

Är det någonting nu när jag har intervjuat dig som jag inte frågat dig om som du hade tyckt det hade varit en relevant att ta upp kring området?

Nej men det som man kan nämna som jag tycker är intressant med det digitalisering det är ju också hur arbeten förändras med digitalisering den kan vara bra att skicka med så där. För att i och med att du digitaliserar en HR funktion till exempel, om det går som det ska och som det tänkt så borde ju alla personers arbeten sen i den gruppen förändras eller hur, för då är ju vissa delar automatiserade det är vissa saker som du har lagt massor med timmar på någon sak och då borde ju det, hur ser vi till att alla är med på det, hur ser vi till att alla får den utvecklingen som dom behöver då och hur planerar man för det skiftet liksom. Den tycker jag är intressant att skicka med. Och en annan sak också som jag vill skicka med det är att om man pratar om digitalisering av HR då tycker jag att det är alltför sällan som man tänker det man ska tänka tycker jag när jag varit inne i såna här projekt att vi kan inte bara fokusera på HR alltså vi måste också ta med ekonomi, IT, kommunikation och tänka mycket mer gemensamt och kan vi göra för våra slutanvändare, våra kunder, så att det är inte det, för dom skiter i om dom jobbar för om dom ska göra något i HR eller ekonomi, dom vill bara ha en smidig vardag och där tycker jag att affärsstöden borde samarbeta mycket mer, det är ett medskick också.

Bilaga C - Transkribering Intervju 3

Vilken är din roll på företaget och vilket arbetsområde är du verksam inom?

Ja, min roll är Workday specialist. Om man ska jämföra det generellt med vilken roll det är på andra företag så är HRIS-specialist så HR-informationssystemspecialist. Uppgifterna är att ta hand om systemet, att utveckla, förvalta och delta i hela digitaliserings roadmap för företaget när det gäller HR och de områdena som är delat mellan HR och IT, HR payroll och HR och andra avdelningar, så det är nästan den sammanfattningen för min roll.

Det är en off-grupp för HR, för koncernen. Koncernen är ett holding företag, inom servicebranschen och som är har kontor i Sverige och opererar i andra länder också och varje land har sin egen organisation och HR och det finns en koncern HR eller grupp HR som kallar vi det är och där sitter jag för att systemet är gemensamt så det är därför rollen är för hela koncernen.

Hur många anställda är ni i er organisation?

Hur många anställda? Jag behöver titta, ja företaget här just nu över 15 000 anställda, exakt siffra kan jag hämta men det kanske behövs inte, och det är det sista som vi har rapporterat är så vi har vi har över 15 000 och vi växer så siffran går upp konstant.

1) Digitalisering

Vad innebär begreppet digital HR för dig?

Digital HR för mig? för mig handlar det om att göra, att ge en HR tjänst till företaget som organisation och till anställda som behöver tjänster från HR på ett digitalt sätt, och när man säger digitalt sätt det är inte bara att använda ett digitalt verktyg. digitala verktyg, det innebär att vi levererar på ett snabb effektivt kommunikativt sätt som når alla och som gör det lätt. Så det digitalisering för mig.

Om vi ska titta HR digitalisering som idé, är det att kunna leverera effektiva tjänster som HR brukar leverera på ett digitalt sätt och med tanke på att det blir lätt och enkelt och effektivt och mer, man kan säga kvalitet, bättre kvalitet på något sätt, för att datorer gör jobbet kanske med mer tillit än människor, dom gör mindre fel ja på något sätt.

Hur arbetar ni med digitalisering på din arbetsplats?

Ja det är i princip att man behöver titta på vad man gör, se om det finns möjlighet att det görs via ett system som vi behöver implementera eller ett system som redan finns och det kan handla om HR processer, så hela en medarbetares resa från att man känner till företaget och kanske skickar en ansökan till något jobb till och med att man blir pensionär eller lämnar till ett annat jobb och kanske efter också. Så det är titta på den här resan med alla delar som finns det och se till att det görs genom digitala verktyg och automatisera processen om det är möjligt och sen också titta på vad företaget behöver från HR som organisation också ser till att det inte görs på papper, det görs digitalt och det vi gör det inte digitalt för att det är kul att göra det digitalt bara. Tänk på att jag kanske inte alls arbetat med papper i sådana steg de senaste åren, eller jag behövde inte arbeta med papper så här sällan, man gör allt genom system, appar och digitala verktyg.

Hur har digitaliseringen påverkat din arbetsroll och dina arbetsuppgifter?

Det har skapat min arbetsroll faktiskt, digitaliseringen. Jag har en del av de här, kanske funktioner, som kanske ska aldrig funnits innan att man har bytt till digitalisering. Och jag är inte säker om det finns någon liknande roll innan att man hade började använda ett system eller en dator, det var i Excel kanske men tror inte att det finns någon liknande som bara förvaltar den här Excel arken men nu det handlar mer om att ny teknologi påverkar min roll, så digitalisering är inte en grej som stannar det är en pågående förändring som händer dagligen i alla områden i alla branscher och det man behöver vara med i princip. Du kan inte pausa din kunskapsutveckling och du kan inte pausa att man söker information och tittar på omvärlden vad händer. Det är en digital roll, man behöver vara aktiv hela tiden det är kanske den mest det mest aspekt i dem här typ av funktioner och roller

Vad använder du för digitala HR-verktyg på din arbetsplats?

För HR, HR plattform core human managementsystem och det förvaltar andra funktioner också genom HR, som är performance, en del av talent programmen, och compensation. Men för att få rätt göra HR jobbet, har vi ett rekryteringssystem som man kan annonsera jobb och samla ansökningar i och göra en sorts arbete med de här ansökningarna och gå igenom rekryteringsprocessen i systemet.

Varje land har sitt eget lönesystem, alla länder har också tidsplanering system för schemaläggning och sådant och det är också, det används inte av HR, det används av verksamheten men är ett verktyg som hjälper med HR-processer vilket är att schemalägga workforce i princip och det finns ett e-Sign system för att hantera digital signering för avtal och allt annat. Det i princip, kan säga det finns många olika verktyg och men behöver och de fungerar. Jag har glömt en av de viktigaste, vårt social och tränings plattform, och det är där vi kommunicerar med våra medarbetare och våra medarbetare kan lägga post och kan lägga inlägg och content och det finns också en del som handlar om kurser och träning. Det är en social och träning och kommunikation och träning plattform. Och de här systemen, de flesta jobbar med varandra det integrerade med varandra, vissa är lite separat och fungerar i sidan men i princip de kompletterar varandra.

Har ni ett team som jobbar med support för alla systemen?

Det är lite olika, det kan vara att jag är inblandad i någon förvaltning för annat system, det kan finnas lokala support för vissa system som har ,man kan säga att support, i den här nuvarande organisationen, de flesta har olika nivåer av support-linjer och det är inte så tydligt beskrivet i vårt företag men kan känna att du har i ett land eller det är ett distrikt, en del av landet, någon som förvaltar och en del uppgifter för ett system och så kan man eskalera frågan vidare vidare vidare till att det hamnar hos de som har de mest ansvar eller de som äger systemet man kan säga de kallas för system-owner eller systemägare i ett företag och den här brukar vara någon person som har ett övergripande bild över systemet, förvaltning, kanske kan sköta avtal med leverantör och allt annat och det är olika, så det finns inte någon struktur bara för att förvalta hur system. Det kan vara för olika som varje system eller ja man kan säga varje del av organisationen.

Vilka utmaningar ser du med digitaliseringen?

Man sitter mycket i webinarer och konferenser just nu och hör av andra kunder och andra företag och organisationer och våra kollegor som vi träffar och jag ska samla och varningar som jag känner och utmaningar som jag får, eller det finns andra branscher som har andra utmaningar för att för att vara ett komplett svar för din fråga.

Utmaningar kan handla om folk som är lite, i varje samhälle det finns en del folk som inte hänga med digitalisering, och det är kanske inte bara en HR fråga, det handlar om banker, HR, alla typer av tjänster som man använder i samhället, att de som inte kan digitala verktyg hamnar utanför och blir svåra att nå och på något sätt och vi tappar de här folk, våra processer. För att de kan helt enkelt inte digitala verktyg. Det kan handla om folk som inte tycker om teknik och digitala verktyg, de kan hamna om deras ålders påverkande, det många olika orsaker. Så det är också den mest utmaning, den mest känsliga grejen med digitalisering. Så man behöver också vara försiktig med hur långt man går med digitalisering och anpassa det, för om man tänker HR, vi behöver ha det i takt med hur våra anställda kan ta emot och digitalisering. Om man tänker på ett teknikföretag, IT företag, de kanske kan gå mer mot digitalisering än att en hospitality eller restaurangbranschen eller är branscher som jobbar med blue collars, man kan säga de som har anläggningar, byggföretag och så. Det är en utmaning som de flesta pratar om.

Den andra är, att också organisationen behöver nyttja av digitalisering samt att en medarbetare behöver nyttja en digitalisering. Jag kan vara en person som tycker om teknik samtidigt är det en tjänst i mitt företag som komplicerar faktiskt grejen i stället för att göra det lättare, som digitalisering behöver riktad mot. Så man behöver också titta på vad nyttan av den här digitaliserings resa som man gör, man behöver spara pengar dit och göra grejen bättre mer eller bättre kvalitet och effektiv och lätt. Om man tar en process eller en tjänst eller något som man gör som HR och det fungerade jättebra nu som jag vill digitalisera och vi hamnar med en jättekomplicerad implementering som medarbetare inte förstår, organisationen nyttjar den inte, så vi har gjort nästan fel, så en annan utmaning är att veta vart man behöver fokusera digitalisering, det är inte än bara att digitalisera allt som man kan. Det finns ju hur mycket som helst.

Den tredje är säkerhet och privat eller persondata och privacy. det är också en tredje utmaning som ja det också känsligt, ganska komplicerat för många, för att det blandar legala och juridiska folk och det blandar verksamhet och operation och alla möjliga avdelningar i och det kostar mycket om man gör fel det och det kostar också mycket om man vill göra rätt för att så att behålla ett företag i linje med GDPR, i linje med lokala lagar och samtidigt vara transparent och effektiv den här balansen med att vara transparent och compliant, är svårt. det kan man göra men man behöver lägga mycket tid och energi och pengar för att behålla den här balansen och för att det inte, vi har en modern tid men man kan ju inte vara otransparent men kan inte behålla allt hemligt, vi har en väl nu när och speciellt den nya generationen som kräver transparens i näringslivet och i organisationer så och samtidigt som man har riktlinjer och lagar och så. Så det är den tredje utmaning.

Skulle du säga att er HR-avdelning har kompetens i att digitalisera HR i den omfattning man gör?

I den omfattning man gör, ja! vi har de som behövs för vad har vi bestämt att göra och det tror jag också dom flesta organisationer har det. För att det också tänk så här, om man behöver nu en talang, speciellt genom digitalisering, det kan man hitta.

Det är hur mycket du vill göra, och hur mycket ett företags ledare och de som fattar beslut har bestämt att göra som är avgörande. Och om man bestämmer att jag vill göra så här, så det bara som du kräver från de som ska göra det, vilket är jag eller min manager på något sätt och är att säga ja det kan man göra men vi behöver hur mycket pengar som helst eller den här summa pengar och det kan man hitta talang och så för att göra det. så att ställa rätt krav som är viktig, men att vi har kompetens ja! för att vi har bestämt göra den här delen av digitalisering eller att rikta oss mot den här linjen. Men om du tänker vad önskar man göra, det är en annan grej och vissa blandar ihop, jag önskar ha allt och att man kan gör allt med en knapp och så ja det kan man göra men det är inte det som vi investerar nu eller det vi har bestämt eller beslutat att göra.

Har ni fått någon utbildning inom området?

Jag ska jag ska skilja mellan systemkunskap och digitalisering som är ett projekt, som en riktlinje som ett företag tar. Ett system de har alla deras egna utbildningar, så HR plattformen har mycket kurser som leverantörer har förberett som de bara man kan göra en ansökan för att göra den här kurs, en del är digitalt, en del är på plats klassrum och en del av webinarer, konferenser och workshops och allt annat och det kan man välja också vilket område av systemet man behöver lära sig.

Digitalisering, nej det finns inget levererat paket faktiskt, det är inte något som man kan bygga en utbildning för det är en mentalitet och ja och mål som man sätter och samtidigt men budgeterar till, rekryterar till, samlar talanger, bygger projekt, startar projekt, är en del av att lära system till en viss personal. Men digitalisering i sig är större än att kan man trycka igenom en kurs eller en utbildning tänker jag. Jag har inte hört om något företag idag som har ett färdigt paket för digitaliserings lärande. Se kan ha som sagt en systemutbildning eller en processutbildning där du gör den här processen genom den här steg och den här kurs eller ett webinar eller workshop som man gör, det är min erfarenhet om det.

Hur har digitaliseringen mottagits i er organisation?

Ja det är efter för det finns en stor efterfrågan samtidigt det är också utmanande när det händer så folk i princip vill ha digitala verktyg och vill ha snabba processer, snabba actions och lätt att göra och så men det gäller att göra det på riktigt när man kommer till en grej. Det man hittar vissa hinder självklart hos mottagare, man kan men behöver också skilja mellan ledare och de som i mitt management delen och de som är anställda och eller de som är på golvet som jobbar. Dem som är, faktiskt, och det är inte kopplat till vårt företag och det är inte kopplat till digitalisering i sig eller branschen i sig, men i princip i alla organisationer det finns en motstånd till förändring och det är en del av kanske alla mänskliga beteenden och tankar så det finns en hinder, ett motstånd till förändring och folk blir rädda från förändring och digitalisering i sig är en stor förändring för alla för att du kommer till en person som är van med en process eller med en uppgift och du tar allt från den här personen och kastar det och lämnade ett nytt verktyg som har inte varit i backend och tittat hur det fungerar och du vill att den här personen läser nu på den här verktyg direkt jag kan förstå hur utmanande det kan vara. det kan vara utmanande för mig.

Om nu jag brukar göra är en grej på något sätt och sen kommer den här myndigheter till exempel till mig och säger nej nu över till det här när du ska fylla den här nya mall och jag ska jag ska säga men det har fungerat tidigare med den tidigare mall varför så ska jag bara lära mig en ny mall, så det är helt är en normal reaktion från en del som blir jätterädda och är lite negativa, nej nej nej nej nej, och sen det finns den här "jag vill ha kul, kul grejer kul grej" de brukar vara de som vi använder för pilot och för att ja göra lite reklam och så får våra för våra verktyg. de är också en jättebra grupp men de är också mottagare till alla så de är kanske inte så kritiska till digitala verktyg och det finns en liten del grupp som är mottagare till digitalisering men har det här tålamodet med att testa och göra kritik och utveckling, kommentar och feedback. så det är olika, men det som är viktig i en organisation är att management, de som fattar beslut, oavsett i vilken nivå, har ett positivt tankar mot digitalisering. Om de som fattar beslut vill inte digitalisera eller att rädda från digitalisering det finns det svårt och övertyga.

2) Informationssäkerhet

Hur arbetar ni med informationssäkerhet på din arbetsplats?

Inom HR, när det gäller system vi är helt beroende på våra IT ansvariga som har folk som har specialiserats mer på informationssäkerhet som ställer krav och gör vad man behöver göra för att säkerhetsställa att alla våra system oavsett om det är payroll, lön, hr, finans, eller de tjänster som man använder i verksamheten. Så det är i princip, och jag tror att alla företag har samma modell, det finns ett IT system som gör det. Och om dom

behöver hjälp från de som är ansvariga för systemet, ställer de krav på oss för att göra sådant som behövs, det är hela tiden dom som har mest ansvar det.

Samtidigt som oss som förvaltar ett system har ett ansvar att säkerställa att vi följer vad deras rekommendation, att vi får den nya till exempel är varningar att det finns ett hot, det som kan hända, det finns andra företag som drabbas av den eller så. Också vår systemleverantör som vi ställer krav på dem och vi väljer hela tiden dom som kan och de som har bra vision i informationssäkerhet och också dom har en del, för du vet nu att de flesta system i världen är moln, så helt enkelt att du har inte något i ditt företag alltså du har här en länk och en inloggning och så det är faktiskt hela data finns hos en leverantör så det är också när våra inköp och legal avdelning, så man behöver ställa rätt krav på leverantörer som man signar med och det tror jag vi gör det bra.

Jag har inte hört att vårt företag drabbats av någon stor händelse eller incident så och men det är ett pågående arbete, det är också att utbilda folk, att väcka idéer eller att väcka konceptet hos folk att du inte behöver öppna varje länk du får och du behöver inte dela information via mejl utan du kan dela inne i systemet. Det är också en lärande resa, att sluta ladda ner och koppla ert mejl och skicka och jag är för allt som är fel adress det skickades till en annan person, det är därför vi har ett system där man kan dela information där inne. det är också mycket åtgärder och information som man behöver uppdatera dom som använder alla verktyg.

Hur arbetar ni med att skapa medvetenhet kring informationssäkerhet i på din arbetsplats?

Det är genom att berätta och göra Sessions, Learning, göra kurser, för slutanvändare och man behöver anpassa den här informationen utskick eller kurs till hur mycket den här personen behöver verkligen. För att en person som är som jobbar i verksamheten, har inget managementansvar, inget HR ansvar, inget finansansvar, han har jättelåg tillgång till information så behöver inte veta mycket om det. Så hög du har tillgång till information, du behöver veta mer och du behöver bli mer medveten. det man gör på många olika sätt, IT gör en del, vi gör en del och i slutet man kan inte säkerställa att alla har på samma nivå, medvetenhet nivå, speciellt när företaget blir så stort och så när man hittar en risk, i vissa fall ska man inte lita på mänskliga medvetenhet, man kan ska ta tekniska åtgärder för att förhindra risken eller den här hot som mot säkerhet. Det är i princip så som man behöver jobba.

Har ni en informationssäkerhetspolicy eller en informationssäkerhet strategi?

Ja, vi har. Och det är alla anställda som läser och godkänner att de har läst våra IT policy och dom som jobbar mer information också, är medveten om den här policy också det är den lokala och europeiska lagar som gäller hela tiden och de rekommendationer som kommer från myndigheter som är ansvariga för den här eller från branschorganisationer som vår arbetsgivarorganisation eller andra. Så det finns och men hur mycket man, ah, de som har en policy behöver faktiskt inte bara läsa och veta att det är den här policyn som finns, man behöver också förstå policy själv.

Så du har en video och du gör många åtgärder för att säkerställa att folk tittar på videon till slutet inte bara klicka på Play och sen okej, och även då vissa bara öppnar video och tittar på något annat så du kan inte säkerställa att folk verkligen läser och om dom läser verkligen förstår och om dom förstår verkligen gör vad policy säger och det är därför man behöver hela tiden uppdatera göra koll att allt som det ska och ja försöka att fräscha upp.

Hur arbetar du med informationssäkerhet i din roll?

I min roll behöver jag hela tiden bli uppdaterat och följa dom här linjer, riktlinjer som finns, sen är det att ha koll genom många olika sätt, på löpande koll, man kan inte gå in i detaljer med varje user men man behöver ha en övergripande koll på hur är läget men hela tiden och uppdaterar eller ändrar, när det behövs, när det krävs, när man känner eller när det dyker upp nya behov. Security framework till systemet och det är ett på många olika set-up som man konfigurerar i systemet för att ge mer access ge mindre access, flytta access eller så, det är också man behöver ha koll på de tekniska delar och det kommer många olika frågor: ”hej jag behöver den här rapport, som Excel”, självklart kan ge är de access till rapporten men kanske behöver vänta för en sekund för att fråga den här personen varför behöver du den här rapporten Excel, ”ja men jag vill veta det här telefonnumret” ja men du behöver inte ladda ner en hel Excel för den här personens telefonnummer. så det är att också vara lite kritisk och lite på något sätt göra lite paus för att försöka ha det om du kontroll eller tiden och det är det pågående arbetet varje dag man får sådana, varje dag och jag tror inte bara jag, vi alla som jobbar med system har den här: ”jag vill ha så här” så kommer det en annan fråga ”varför börja det logga ut efter några minuter, jag behöver ha inloggat hela tiden”, ja men varför? ”ja men för att när jag lämnade dator, behöver jag vara inloggad”, ja så du lämnar datorn inloggad öppen när du går. Så om du börjar ställa frågor om grejer på folket, upptäcker man att och folk behöver vara med medvetna om grejer, ja det händer inte varje dag men nej man kan säga att ja att vi har kontroll varje dag, försöka att hålla det under kontroll, är en grej som jag gör i min roll dagligen nästan.

Har ni fått någon specifik utbildning i hur ni ska arbeta med informationssäkerhet just i din roll?

Inte i informationssäkerhet i allmänt, jag har fått en del utbildningar som gäller Security fault framework i vår HR-plattform som jag är ansvarig över och jag har allmänna information angående IT-säkerhet och ja allmänna IT-frågor i princip, på grund av mina tidigare erfarenheter i liknande uppgift, jag har jobbat med system för länge och lite intresse också. För mig, för min roll, och de flesta som förvaltar ett system i sig, då behöver inte så mycket IT, informationssäkerhet för att det där IT lägger deras kontroll och ditt jobb börjar efter, inne i systemet och där behöver du veta mer om Security framework inside the system, och där är jag nästan trygg med det och jag har fått utbildning som behövs som finns, från de som har byggt systemet. Stora förändringar eller utmaningar, hela tiden kan man gå tillbaka till systemleverantören och ställa rätt krav eller uppdatera eller be om hjälp.

Vilka utmaningar ser du med hur ni arbetar med digitalisering kopplat till informationssäkerhet?

Ja, det är ett inte en utmaning, kanske jag över oro, men inte oro men, man behöver veta att cyber attacker, cybersäkerhet är framtid och är ett ökat hot och risk i hela världen, kanske i Europa mer än andra delar av världen, och det ställer mer krav på oss som jobbar med det, på vår IT, på alla som arbetar med det, att ja ett fel blir mer och mer och mer farligt dag efter dag för att vi har mer och mer beroende på digitala verktyg.

Hur påverkade införandet av GDPR-lagstiftningen ert arbete?

Allt, det är ju den största förändring för vår datahantering kanske i Sverige sedan de här infört PUL, som är nu överskrivet av GDPR på något sätt. Det handlar om allt, och det är en öppen riktlinje, så det är inte direkt anpassat för Sverige på något sätt och inte anpassat för en speciell business, det är en stor mentalitet förändring som kräver ett kontinuerligt arbete för att vara compliant, det är en resa och en kontinuerlig resa som man behöver som var med. I varje del, behöver man ställa samma fråga, behöver vi all den här informationen ja eller nej, behöver jag spara den här informationen ja eller nej, behöver jag dela den här informationen ja eller nej, hur länge behöver jag spara det och vem ska ha access till och vad händer när det inte behövs och hur man raderar och hur ofta. De här frågor, gäller varje värde i våra HR-data, så det påverkar alla processer, alla rapporter, all datalagring, det är också en mentalitet förändring för oss och för dem som vi jobbar med.

Upplever ni att det finns en risk eller utmaning med att obehöriga får tillgång till känsliga data i samband med att man digitaliserar stora delar av HR-processerna?

En risk, det är väl det hela tiden, samma risk. Det finns ingen ökad risk kan jag säga, men vi håller samma nivåer och faktiskt behöver kontrollera, kontrollera, kontrollera. Om någon gång det händer att någon del av information läcks till obehörig, det kan hända, men vi vet inte hur och när, annars hade vi vidtagit åtgärder. Det kan hända att någon laddar ner en rapport och i stället för att skicka det till Louise Wetterlundh med två t skriver man adressen fel, det är så lätt. Det kan vara en inom en organisation, men kan vara utom en organisation, kan ha olika leverantörer kopplingar integrationer och så och det kan börja så.

Det är en risk som det finns hela tiden och du kan förhindra hur mycket som helst men det kan inte göra det noll. Man kan tänka på de stora, stora, stora frågor cyber attacker och så, risken finns, vi har ett dagligt arbete för att det inte händer och vi försöker att det blir mindre risk och att det inte händer, men risken finns och risken finns hos alla. Vi har hört mycket berättelser om andra företag i Sverige och utanför Sverige, som har drabbats av att en miljon kunduppgifter har läckts på den här företag och en halv miljon uppgifter har läckt på den andra företag. Det är en grej som man tänker på när man arbetar hela tiden, att inte göra det lättare för HR-data blir i obehöriga händer.

Om det sker en informationssäkerhetsincident i er organisation, hur arbetar ni med att hantera det?

Om det skulle hända, det ska, jag vet inte ja, det här inte hänt så jag vet jag kan inte berätta exakt hur det kommer och fungera. Men om något händer, är det en kris som företaget ska hantera genom deras krishantering policy och GDPR-policy och datasäkerhetspolicy. Jag tror att de finns hos IT och där dom ska ta fjäder för att fortsätta nya arbeten med incidenter. Jag har själv inte varit på någon sådan, och även om det händer det är inte jag som driver en respons på något sätt. Det finns många olika *** över och IT som legal kommunikation som arbetar tillsammans kanske jag en del. Det är krishantering, dataläcka är inte någon lek.

Det var faktiskt dom frågorna jag hade finns det något som nu när vi har haft vår diskussion som du skulle vilja tillägga som du tror hade bidragit till studien?

Inte så mycket att tillägga, du har tänkt en stor del av de frågor som nu cirkulerar i vår bransch och vårt arbete där det jag kan säga att HR som funktion är inte så olika än de andra. Vi har samma risker samma utmaningar som finans, som verksamhet och operation och andra delar med informationssäkerhet och med digitaliseringsresan men det som gör HR annorlunda är att det påverka våra anställda, så det är hela företaget, en organisation i sitt core är en del medarbetare tillsammans. Det är inte är datorer och bord och stolar, det är folk

som arbetar tillsammans ett gemensamt mål och det påverkar dem direkt. det är kanske det som gör det annorlunda eller kanske mer känslig eller farligt på något sätt, det är det som jag kan tillägga.

Bilaga D - Transkribering Intervju 4

Vilken är din roll på företaget och vilket arbetsområde är du verksam inom?

... det är mer handlar om att vara förvaltningsansvarig för HR-IT system och det betyder att jag egentligen varken är sitter på HR eller IT även om jag organisatoriskt hör till HR så är det ju någon slags hybrid, lite grann.

Skulle du kortfattat kunna beskriva ert företag?

De är verksamma inom bank och försäkring och väldigt decentraliserat.

Hur många anställda är ni i er organisation?

Strax under 10 000

1) Digitalisering

Hur arbetar ni med digitalisering på din arbetsplats?

ja det beror ju på vad man menar med digitalisering det här kan ju betyda jättemånga olika saker för olika personer men det man har gjort är ju då att implementera ett vad vi kallar för medarbetarsystem eller om du vill HR-system, gemensamt. Där det är mycket både då vad som kallas för en employee self-service och manager self service det vill säga att man själv som medarbetare eller chef går in och gör vissa saker i systemet. Det är därför vi kallar för ett medarbetarsystem så det är ju ett steg att bli mer digitaliserade men... och det är ju det som berör mig.

Men digitalisering är ju så väldigt mycket mer än det men så att det är svårt för mig att säga hur företaget jobbar med digitalisering för att det finns egentligen inte så mycket samordnat, det kanske det gör, men inte som jag ser. Men inom HR området så är det framför allt det här systemet då som står för mycket av digitaliseringen och även att vi försöker använda den aggregerade data vi har för att så småningom kunna ta mer informerade beslut men där ligger vi bara i startgroparna och då jobbar mer med Analytics och sådant

Hur har digitalisering påverkat din roll och dina arbetsuppgifter?

Ja, jag har jobbat med det här sen 2010 i olika företag och det är ju det jag gör om man med det menar att se till att det finns IT stöd för HR processer, om det är det vi menar med digitalisering då är det jag gjort i av 12 år.

Vad ser du för utmaningar med digitalisering?

Utmaningen är alltid är att få engagemang, alltså förändringsledning, change management, att få folk att förstå varför dom ska ändra arbetssätt och då menar jag inte bara chefer medarbetare utan även alla inom HR. Det handlar också om att ofta så implementerar du system som stöd för processerna och då om det är stora företag med många lokala avknoppningar så måste man kanske se över och börja jobba mer likartat och det är en förändringsresa som kan heta duga i vissa fall för att det kan vara jättesvårt att få folk att ändra sitt sätt att se på sina processer. Alltså det är väl de som jag skulle säga de absolut största utmaningarna.

Vad innebär begreppet digital HR för dig?

Jag använder aldrig det uttrycket så jag vet inte egentligen vad man menar med det faktiskt, jag kan inte svara på det.

Vad använder ni för digitala HR-verktyg på din arbetsplats?

Vår HR-plattform, den inkluderar ju i stort sett alla processer. Så självklart, ett lönesystem det har man ju, det har ju alla för folk ska få betalt och utöver det så är det då ett system så för alltifrån att hantera själva anställningen till rekrytering, onboarding, offboarding och lärande, prestation, mål, så att det täcker in inte alla men de allra flesta processerna i samma system.

Skulle du anse att organisationen har tillräcklig kompetens för att hantera digitaliseringen inom HR?

Ja men det tror jag, från medarbetarna och chefen sett håll ja, sen om organisationen är redo för det, det är ju en förändringsresa här också. För det är en stor skillnad att jobba med den här typen av molntjänster, eller SaaS tjänster som det egentligen är så krävs en helt annan typ av förvaltning en helt annan typ av rolluppsättning på företaget både på IT och på affärssidan då, i mitt fall hr, men det skulle lika gärna kunna vara en någon något annat system, någon annan affärssida. Det krävs andra roller än vad man är van vid och också nya rutiner så att det, på det här företaget så har ju den resan ganska nyligen startat jag tror man började jobba med den här typen av tjänster och eller system kalla det vad du vill, ganska nyligen för bara dryga året, sen medan där jag jobbat tidigare så har ju den som pågått i över 10 år.

Hur har digitaliseringen mottagits i er organisation?

Men jätteblandat, återigen gå tillbaka till förändringsledning, jag skulle säga att mottagaren av det, så länge dom får ett stöd som är bättre än vad de haft innan och de förstår varför de kanske måste ändra vissa rutiner så skulle jag säga att mottagandet välkomnas och allt som gör din vardag lättare och det är ju det som är syftet. Sen om det gör det alltid, säg det, det kan ju ifrågasättas men jag skulle säga att det till allra största grad så gör det och så länge folk ser att jo men det här funkar mycket bättre än det jag hade innan, man kanske till och med går från papper till att få systemstöd och då är det ju jättepositivt. Däremot så kan det ju innebära mer krångel ibland för administratörer på i det här fallet och hr så kan det ibland till och med bli mer jobb och det är ju inte alltid roligt så.

Har ni jobbat någonting med att utbilda personal i de här systemen?

Nej inte utbilda man kan inte göra klassrums utbildning eller traditionell utbildning inte ens vare sig digitala eller klassrum på den här typen, när man är så många som vi är utan det handlar om att du har kontaktpersoner för de olika processerna som i dom respektive bolagen så säger att vi har 25 lokala enheter så ska vi varje enhet har en person som är ansvarig lokalt för sin process i systemen och då är det dem man ser till att man utbildar och håller informerade. Och det här är ju en ständigt pågående process för det förändras ju hela tiden, det kommer nyheter, det kommer uppgraderingar, man ändrar, man skruvar, man förbättrar, så du är ju aldrig klar med när du jobbar med SaaS tjänster utan det är ju ständig ständig ständig förändring och då gäller det att man hela tiden, att man bygger upp en förvaltning så att du hela tiden har en kommunikation med dem som är lokalt mottagare som sen då väljer hur dom utbildar. Är man 50 så kanske man samlar alla över en fika och berättar, är man 300 så kanske man skickar ut ett mejl eller lägger ut någonting på intranätet eller vad man gör, men det brukar sällan centralförvaltning lägga sig i för att det i alla fall i den här typen av större organisation, det går inte. Utan man ser till att det är lite train to train tänk då även om vi inte skulle kalla det.

2) Informationssäkerhet**Hur arbetar ni med informationssäkerhet på din arbetsplats?**

Ja jättemycket, det finns ju otroligt mycket människor som jobbar med det som sitter på IT, jag sitter på HR, har ju med dom att göra men det jag sitter ju inte i den organisationen men det här det är ju ett av våra absolut viktigaste områden med tanke på vår affär så att säga.

Har ni en informationssäkerhetspolicy eller informationssäkerhetsstrategi?

Ja

Hur ser arbetet ut för att etablera den?

Alla medarbetare måste gå flera utbildningar som handlar om informationssäkerhet årligen så att det är obligatoriska utbildningar både som nyanställd och sen måste den uppdateras minst en gång per år och det är inte bara en utan det är flera olika.

Arbetar du med några särskilda säkerhetsrutiner i din roll? Hur arbetar du med informationssäkerhet i din roll?

Nej egentligen inte mer eller ja det gör man ju alltid alltså det är ju de här bas grejerna som är superviktiga att vad får man göra, vad får man printa, vad får man maila, var får man, hur får man hantera data, men det men det börjar ju sitta i nästan i ryggmärgen det är ju ingenting som man ens tänker på längre för att nu är GDPR så pass etablerad tror jag för alla som jobbar med det här, så att det behöver man inte ens tänka på, det ligger där liksom det är som "bread and butter", det måste du ha koll på såklart så att självklart jobbar vi med det hela tiden men det är så inarbetat i rutinerna att du nästan inte ens tänker på det längre skulle jag säga i alla fall dom som jobbar så pass mycket i system som mitt team.

Hur många är ni i ert team som jobbar med det?

6 som jobbar med central förvaltning

Har du och ditt team fått någon särskild utbildning eller idag i inom informationssäkerhet och hur ni ska jobba med informationssäkerhet i era system?

Ingen kanske officiell utbildning, självklart är det någonting som vi pratar om, och vi tar upp det med jämna mellanrum och påminner oss själva och varandra och vi pratar om när någonting kanske, för det händer ju att man upptäcker att någon ändå har slarvat lite eller slipped liksom och då tar vi upp det och diskuterar det. Men nej jag skulle inte säga att vi har fått en regelrätt utbildning så att vi kan visa upp det här har vi ett diplom, check på den, men det är som sagt ett ständigt närvarande ämne.

Om det sker en informationssäkerhetsincident i er organisation, mer specifikt er avdelning, hur arbetar ni med att hantera det?

Beror alldeles på hur allvarligt det är. Vi skriver alltid en rapport och den skickas till chef som sedan avgör om den ska skickas vidare till datasäkerheten eller IT-säkerhet beroende på alldeles beroende på. Men vi skriver alltid en incidentrapport på oavsett vad det är men och väldigt ofta är det så pass begränsat och smått så att det inte blir någon stor grej av det men det händer ju att det skickas vidare då och då finns det ju processer och rutiner för det så att ja det är väl så de flesta företag gör skulle jag tro.

Ser du någon risk med att så mycket data om dina alltså era anställda förvaras i ett moln?

Nu frågar du mig och då säger jag absolut inte. Frågar du någon annan här som sitter med IT-säkerhet skulle dom kanske var lite mer tveksamma, det vet jag inte men nu utgår jag bara från mig och jag hävdar med bestämdhet att den säkerhet som finns kring de här stora leverantörerna av molntjänster, dom säkerhetsspärrar som finns kring vår data skulle vi aldrig kunna göra själva, aldrig, vi har inte de resurserna. Här pratar vi ju liksom, det finns ju ett par stora leverantörer och dom hanterar ju data för otroligt många företag, har hela avdelningar som inte gör annat än att se till att data är säker därför att det är hela deras business handlar om det. Jag tror inte att vi någonsin skulle kunna ha varit i närheten av den säkerheten själva så att jag är inte ett dugg orolig men det finns fortfarande absolut oro och man ska vara man ska naturligtvis tänka till och vara försiktig och man måste se till att man har rätt leverantörer och att man har rätt typer av avtal och sådana saker men går man med någon av de här riktigt stora leverantörerna så tycker inte jag att man behöver vara orolig men det är min åsikt, inte företagets åsikter.

Ser du några andra utmaningar med att digitalisera HR kopplat till informationssäkerhet?

Gör jag det, alltså nej egentligen inte, men jag kanske är jag är ju färgad av det här som jag håller på med så länge så att nej jag kan inte säga att jag gör det inte jag nej.

Hur påverkar det införandet av GDPR ditt arbete?

Men jättemycket, framför allt oron innan, osäkerheten, som ju var massiv det var ju in i det sista så är det ingen som riktigt visste och kanske egentligen fortfarande inte riktigt vet hur allting ska tolkas som det är, egentligen vet man ju inte det för att det ställs på sin spets och det hoppas man ju att det inte ska. Men ja just när det hände så dom åren före under och efter var ju lite hysteriska skulle jag vilja säga och det var ju på gott och på ont det behövdes kanske, bra att någonting sågs över men just den här osäkerheten var väldigt onödig, det hade kunnat varit mycket tydligare regler.

Men sen är det ju också i vissa fall kanske det tagit lite tid att det släpat efter med tekniken ibland att dom här större leverantörerna då måste ju uppdatera så att det går att följa lagarna och det har dom ju gjort men då har liksom dom har varit... När, dels vi vet inte riktigt vad som krävs, vi vet inte riktigt vad leverantörerna kommer tillhandahålla för möjligheter, vi vet inte vad vi har för interna krav, så ja alltså allting rörde sig runt. Det var ju lite kalabalik skulle jag vilja säga, var känslan där under några år. Sen nu har det landat, nu är nu är... tror jag både dom som är dataansvariga och vi som sköter systemen och alla känner sig lite lugnare och tryggare vi tror att vi har våra tolkningar som vi tror på och så där så att det känns liksom, nu vet man mer, men det är ju fortfarande... min tolkning, är att det är ju fortfarande liksom ingen som 100 % kan säga exakt vad som gäller utan det är ju varje företag gör ju sin tolkning och det kan jag fortfarande tycka är väldigt olyckligt men det är ju som det är.

Finns det något du vill tillägga kring ämnet och det vi diskuterat?

Nej men jag tycker att du har ställt bra frågor är relevanta och bra och jag tror också att och det har du säkert märkt att du kommer få jätte olika svar beroende på vem du frågar och framförallt vilken roll personen har som du frågar och det kan jag tänka mig superintressant är lite avundsjuk på dig som får sammanställa det här, jag hoppas att du också pratar med några DPOer, data protection officers, och får deras tänk på det för att den det kan nog skilja sig och sen tror jag det skiljer sig jättemycket på olika för industrier alltså vilken typ av företag man pratar med.

Bilaga E - Transkribering Intervju 5

Vilken är din roll och vilket arbetsområde är du verksam inom?

I min senaste roll var jag global head of HR-operations i ett amerikanskt företag. Idag arbetar jag som konsult, vilket betyder att jag jobbar med olika företag, HR-processer, HR-transformation.

Kan du kort berätta om det tidigare företaget du arbetade på?

Det var ett företag med indtil 55 000 medarbetare så ganska stort företag. Så jag gjorde en global HR-teknologistrategi, omkring att göra jobbstruktur, karriär, career structure for de olika typer av jobb man har, implementering av HR-system, men också roles and responsibilities, HR-processer och HR-datasäkerhet. Men jag satt ju på HR sidan, så mycket av det tekniska ansvaret, till exempel det tekniska ansvaret på IT-säkerhet, det satt på IT avdelningen. Så jag arbetade väldigt tätt ihop med IT om säkerhet. Så på HR-sidan var jag den som gjorde policys på hur man gör ting. Det var mycket med vilken typ av data kan man ha tillgång till med de olika rollerna man har, och att man också begränsar så att det endast är tillgång till den data man har behov av som en person får tillgång till. Och det var också en del kring GDPR. Och som ett globalt företag så hade vi också det som heter Data Transfer Agreements, när det exempelvis sitter en HR person i London men som jobbar med en medarbetare som sitter i Tyskland eller frankrike eller sverige och faktiskt om man gör en anställning av en person i Tyskland men man sitter i London och gör det, så sker det en data transfer...

... jag har sett företag som jobbat i Scandinavia eller europa, är det inte många som känner till data transfer agreements, för de har inte tänkt på dem, men om man ska uppfylla de legala kraven inom EU exempelvis, då måste man ha data transfer agreements, man måste ha ett legal foundation för det man gör. Men ständigt ser jag många skandinaviska exempelvis danska eller svenska företag som inte känner till och de har aldrig gjort det, de har inte tillräckligt internationell erfarenhet för att tänka på det. Men asså som globalt, hade vi en hel standardprocess för det, varje gång man hade en legal entity i ett land, så ska det finnas en data transfer agreement för att man ska ha lov att tillgå personaldata i den legal entity.

2) Digitalisering

Hur arbetar du med digitalisering i ditt arbete?

Många verksamheter och företag som jag jobbat med, internt eller externt, så är digitalisering väldigt ofta att "man sätter ström til processen" og det var så det var, och det var lite synd faktiskt. För de, så tänker man, att man har processen, den är redan beskriven så för man bara processen in i systemet, man tänker inte på hur man kan vara färdig med att göra processen på det sättet. För det är ofta man gjort processen på ett sätt för det var det som var bra, men när man har digitalisering och när man har data tillgängligt kan man faktiskt göra processen på ett annat sätt.

Jag vill gärna ge dig ett exempel: när man sitter på performance management eller performance and development som har verksamheten ofta processer med annual process och så gör man goal setting i januari, och så gör man kanske kvartalsvis eller halvårsvis så gör man en review och uppföljning, med hur går det, hur mår du, hur går det i förhållande till dina objectives. Så lägger man in att man har uppföljning var tredje månad eller var sjätte månad, men det är ju en process som om man inte har ett system. Så lägger man bara in det i ett system. Det är som man faktiskt gärna gör med processen det är att ha diskussionen med medarbetarna var de vill med sin karriär, om de tänker på, om de är nöjda med det som dem gör, om de tänker att de vill ha någon förändring eller såhär, men i ett företag, vad jag minns, där jag var Head of HR-operations, så gjorde vi en analys på vår HR-data, en survey på medarbetarna för att finna ut när de har behov av att diskutera karriär, och det är inte en gång var tredje månad eller en gång var sjätte månad, faktiskt så fann vi ut att då personer har behov, och har mer behov av att tala om sin karriär, det är exempelvis om de varit på semester, 2-3 veckors semester, och när man kommer hem från så semestern tänker man på sin karriär, så när man kommer hem från semester är det bra tid att ta karriärnsnack med medarbetarna för det är det de tänker på. Eller om man har en peer, kollega i sitt team som ska lämna sitt team, som blir transfered, promoted eller slutat jobba, så tänker man också på sin karriär. Eller om man får en ny chef, om ens chef blir utskickad (***) så tänker man också på sin karriär.

Så när man tittar på system så kan man se någon situation där medarbetaren (***) för de tänker på sin karriär mer än på andra tidpunkter. Men det är ganska synd att verksamheterna använder den här funktionen, för de skulle man normal, det skulle exempel vara i en organisation en manager, det här är en bra tidpunkt att diskutera karriärer med medarbetaren för det är (***) eller något. men det är ganska synd att man gör det. Man har en gammal process som man lägger (***) till och det har jag, inget som jag som konsulent jobbar med att

försöka vart kan man få HR processen att spela ihop med detta system. så man inte bara sätter ström till processen. Man uppfinner, man gör en ny process för då har man väldigt mycket information. Och det tror jag är det som sker i nästa åren. Man gör lite re-invent, man gör nya processer, för nu har man data och har mycket mer (***)

Vad ser du för utmaningar med digitaliseringen?

Ja asså, jag faktiskt väldigt beestrad på digitalisering, men utmaningar, det är ju kanske lite att många personer är olika, och det är ganska många personer som ständigt tänker på att införa exempelvis Performance Management, att (***) vänder sig till, man uppdraget till att det ska vara annual goal setting, quarterly review with your employee, och så vidare. man har vant sig vid hur saker ska vara och de tänker jag faktiskt blir en utmaning att de stora HR systemen de, gör repeat på det som är de gamla processerna, och de är inte så innovativa. Så faktisk blir det några problem att, nu har man de här stora systemen och stora processerna i systemen och jag diskuterar ofta med andra konsulter som säger att ja vi vet hur Performance Management är, och systemen (***) Performance management, men det understöder de gamla sätten av Performance Management. Så faktiskt upplever jag lite att innan vi hade computer systemen så kom man ju finna ut hur man skulle göra ting, men computer systemen berättar hur vi ska göra saker, så vi är i en situation där computers, system, processer, de sänker oss, de sänker farten, för de känner bara (***) vi måste göra det på det sättet som systemet vill att vi ska göra det. Så computer system gör det möjligt men är ofta också en begränsning för innovation.

Vad använder du för digitala HR-verktyg i ditt arbete?

Jag jobbar med olika verksamheter, och jag jobbar mest med success factors, så flera av de stora företagen jag jobbar med använder success factors. Men faktiskt så försöker jag göra mitt jobb independent av HR-system. Men det som jag jobbat mest med har varit success factors, och det gamla systemet kinosoft, som är ett väldigt gammalt system, så har jag jobbat lite med workday och sen har jag jobbat med ganska små system, greenhouse, (***) growt, amature, cornerstone. Men mest success-factors.

Upplever du som konsult, när du kommer ut i organisationer, att de har den kompetens som krävs för att digitalisera HR?

Nej, faktiskt upplever jag i två av de projekten jag jobbar med just nu, de organisationerna har implementerat HR-systemen, och så har de inte haft tillräcklig kompetens, så de har bara implementerat de IT konsulterna har sagt, det är så här man gör, i success factors gör man så här, och så har de implementerat de och så fungerar det inte särskilt bra. Man ska också tänka på att om man exempelvis implementera Performance Management, så får man ställa fråga, vad är Performance, vad är performance för oss, vad är performance för denna organisation. Och det glömmar de att fråga om, utan de tänker att nu implementerar jag ett performance management system och så kommer allt bli bra. Det som jag upplever är att man litar lite för mycket på IT konsulterna och IT systemen, så glömmar man att fråga vad det är man (***) sin HR-strategi och vad man vill med sin HR verksamhet.

Hur upplever du att digitaliseringen mottagits i de organisationer du är ute i?

Jag men faktiskt så tänker jag att man tittar på det ganska optimistiskt, men tänker man ser inte, ja man tänker att IT-system löser ting, och så tänker man att det går ganska lätt och att man inte behöver göra något jobb själv. Så i första omgång blir det mottaget ganska positivt och man tänker, jaja, IT systemen löser det, men så har man implementerat det, och så finner man ut att man at man inte är self service och så vidare, det fungerar inte om man inte tänkt på hur man ska göra det. Så i första omgången är man väldigt optimistisk och kanske lite naiv, och i andra omgången blir man så förtvivlad eller skuffet över den upplevelse som man har.

3) Informationssäkerhet

Hur arbetar du med informationssäkerhet i din roll?

Ja alltså nu mycket som konsult på HR processer, så det som jag hjälper mycket till är att säkra mig att när vi gör en HR-process är att vi också diskuterar de här rollerna som är involverade i processen. Det första är att man begränsar hur många som ska vara med i processen för det är ganska ofta så ser man att i verksamheten så finns det två eller tre eller fyra approvals på en process men det är ju folk som sätter kontroller och det gör at för det första sprider man data så det är ganska mycket folk som är med, och som har tillgång till data och nummer två är att det ansvar eller om det är 3 eller 4 personer som ska godkänna det som man gör, vem har egentligen ansvaret för det man gör. Så där prövade vi är säkra mig at man begränsar responsibility at man har, who is responsible, who is responsible for this, and who really needs to approve. Så att man begränsar det så mycket som möjligt, vem som har ansvar och vem som har möjlighet och tillgång till at godkänna det. Och så

selvfølgelig att de här rollerna är bra definierade så att man får begränsad tillgång till deras (***) så mycket som möjligt.

Eller så kan jag kanske säga att på det andra sättet är jag ganska mycket fortaler för transparence, och jag har jobbat i en organisation hvor vi gjorde salary rates, eller salary ranges, och där fick vi lagt ut dem här salary ranges med job level på intranätet, på verksamhetens intranät eller sharepoint. Så medarbetarna kan se om man är level 7 eller level 9 eller 11 eller någonting, så kan man se hela rangen vart man är. Så hela politiken, rewardspolicy, så hela den var lagt ut på intranätet, det var inte spec kring lön på personer, men att politiken kring rewards är så transparent som möjligt. Det är viktigt synes jag för det hjälper att skapa transparens och skapa rättfärdighet och fairness i organisationen.

Har ni fått någon specifik utbildning i hur ni ska arbeta med informationssäkerhet just i din roll?

Ja det var en bra fråga, nej, jag har tagit interna kurser i informationssäkerhet, och så har jag varit på kurser från två HR-systemvenders i informationssäkerhet, så har jag tagit GDPR kurser alltså europeiska datasäkerhetskurser. Men jag har inte någon en skola, eller universitetsutbildning.

Vilka utmaningar ser du med hur ni arbetar med digitalisering kopplat till informationssäkerhet?

Det er alltså det gör jag ju lite, speciellt vill jag säga som jag nämnde tidigare med mindre företag, det finns ganska många mindre företag som jobbar med HR och känsliga data men inte känner till speciellt mycket om internationell law, så det gör ganska mycket ting som de inte har lov till att göra och det är hela tiden. Och det är inte tillräckligt med, Outlook exempelvis, i outlook så kan jag sända, så kan jag lave att sende ett attachment som har känsliga uppgifter i det här attachment, och outlook gör inget för att hjälpa mig att se att här skulle det finnas ett password eller här skulle det finnas någon säkring eller någonting, så det tror jag är något systemen ska vara bättre till att känna igen, och se här, oj du har ett attachment, det ser ut som det här attachment har känsliga uppgifter, vi ska inte göra ett password eller göra någonting åt det här dokumentet. Där tror jag systemen ska bara lite bättre för vi delar mera och mera uppgifter, och vi är inte helt uppmärksamma på det vi gör och vad vi har lov att göra.

Hur påverkade införandet av GDPR-lagstiftningen ert arbete?

Inte så mycket nu här, men i mitt förra jobb som globalt ansvarig för HR-operation då var det en ganska stor del, så jag jobbade tätt in på vanlig HR, HR-policy department, med IT och med legal, om att göra ett helt framework, som vi hade, ett globalt framework för att säkra oss att hela organisationen globalt blev GDPR compliant, och jag var då ansvarig för HRD, men det är mycket, GDPR är mycket mer än HR-avdelning med där satt jag med ansvar för HR. Jag har i de sista två åren inte gjort någon GDPR relaterat. Ikke andet, Jag har jobbat med ett företag som gör leadership assesment, och leadership development, och när man gör leadership assesment så har man ju också känsliga uppgifter, och där hjälper jag mycket till att få, det var ett litet företag, där hjälper jag också till att få implementerat några basic principles som är omkring IT-security och IT.

I de organisationer du jobbar i, och även din tidigare arbetsplats, har ni arbetat något med en informationssäkerhetspolicy eller en informationssäkerhetsstrategi?

Nej, det är inte den typen opgaver som jag har varit involverad med, men jag har jobbat med HR-processer, asså jag har jobbat tätt ihop med HR-folk och inte så mycket med IT och security. Men faktiskt har jag just i sista veckan talat med en kollega från min firma och han jobbar med cyber security. Så mitt företag har en avdelning som jobbar med cyber security och det gör dem inom IT men där har dem ofta inte personer med som känner till HR-strategier och HR-operations. Så vi talade faktiskt nu i veckan om att vi ska göra fler samarbeten. Sådan att man gör samarbeten ihop med cyber security och HR-operation HR-teknologi, så man får kombinera de här två kompetenserna. Så kanske mer av det i framtiden tänker jag.

Upplever du att det finns en risk eller utmaning med att obehöriga får tillgång till känsliga data i samband med att man digitaliserar stora delar av HR-processerna?

Ja, jag känner till ett tillfälle som exempel när coca cola gjorde compensation planing, och då var det en medarbetare i USA som hade allt compensation, allt globalt, på hans computer, och så blev hans computer stulen, och så var det en som fick fat i global compensation data för hela coca cola så det är stadigvæk och jag har också sett i ett företag där jag jobbat med var de gör compensation planering i ett excel ark och där de sende ut excel-ark och så skriver folk tillbaka i excel-ark utan lösenord, och så ligger det compensation data för tusentals personer i emails, så det ser jag stadig, och jag tror det finns en maturity level eller kompetente inför det området det är stadigvarit något som ska bli mycket bättre och folk är lite för naiva tänker jag och man tänker inte tillräckligt på säkerheten. Men när man använder IT-systemen, så tänker man att IT systemen redan har gjort allt det, men det har systemet inte om inte man gör en bra process.

Om du i din roll upplever en informationssäkerhetsincident, hur arbetar du med att hantera det?

Vi har faktiskt på min telefon och min computer där har vi att det står när jag startar min computer så står numret på får IT-desk om man har security incident, så jag jag har blivit tränad i vår security policy så om man upplever något som har hänt så känner jag till processen till det nummer jag ska ringa. Så antingen sender jag ett email eller ringer till ett nummer men där har vi support 24/7 på det om det sker någon incident. Så vi känner till de stegen vi ska rapportera om det här.

Finns det något du vill tillägga kring ämnet och det vi diskuterat?

Nej alltså, det är kanske lite omkring hacking, alltså det som också händer, för det vi har diskuterat det är lite kring min kompetens och min erfarenhet, men det man också upplever är faktiskt hacking. I min firma där jag var i USA där upplevde vi hacking var några personer de fick tillgång till en profil på en medarbetare i (***) kontoret, genom hacking. Och så kommer de in i systemet. Och det är något, det var ett ganska stort företag så vi hade en bra process för att hantera det men hela frågan kring hacking, det är något som efter det, när jag kom hem till europa och kom hem till danmark, där ingen talar om hacking, folk tror inte det finns till. Det är ett ting hur man bekyddar sin data men ett annat ting är hacking, hur man upptäcker hacking, the stains från hacking, för det händer också. Det är ett område som man inte har så mycket kännedom till eller bevitnat så.

Det vi gjorde faktisk efter vi hade haft en hacking var att vi gick in och tittade på hur vi kunde förbättra att om en profil bliver stulen, att någon får tillgång till din profil så då gjorde vi som att vi fick bättre tillgång till att se vad denna profil har gjort, vad denna profil har tillgång till, så att vi får se en bild på vad som hänt. Och via det kunde vi faktiskt så kunde vi också gjort en process om en profil gör sådan och sådan sådan så är det misstänkt så ska vi se mer på det. Så vi tog faktiskt en specifik hacking och så fick vi defintierat några av de tingen, och så fick vi faktiskt definierat en monitoring process som tittar på om någon bestemete ting finns där så är det möjligtvis en hacking. Så kunde de öka bevakningen och finna ut när det händer ting.

Bilaga F - Transkribering intervju 6

Vilken är din arbetsroll?

Serieentreprenör, jag har inte gjort annat än varit byggt bolag de sista dryga 20 åren men inom cybersäkerhet.

1) Digitalisering

Hur arbetar ni med digitalisering i din roll?

Ja, jag drar ju nytta av att vi har en ganska långt gången eller pågående digitaliseringsprocess. Det finns det finns ju olika digitaliseringsindex, det mest vedertagna där har ju Sverige alltid legat trea 4 och femma, brukar vara Singapore USA som byter lite grann plats och så här och så ligger Sverige trea fyra femman kanske och men det är viktigt att poängtera då att det här är det här är alltså det digitalisering sätt relation till alla andra. För det är ju så om du säljer om du säljer så här trådlösa hörlurar i en butik och sen lägger du ut det på nätet, det är ju en digitalisering, men det är ju inte det som jag egentligen menar med digitalisering, det är när du helt och hållet kan förändra dina verksamhets- och affärsprocesser och göra något helt annat på ett helt nytt sätt och där är vi ju inte än, nästan ingen är där.

Men vi kan ligga 4 eller femma i digitaliseringsindex men det betyder ju bara att vi ligger 4 eller femma bland alla andra som är ganska dåliga på det, och nu så kommer vi då till svaret på din fråga, det finns också ett väldigt välkänt och välanvänt cybersäkerhet- och informationssäkerhet index och där ligger Sverige just nu på 41: a plats och det är ju obra får man lov att säga. För att om du ligger på 100:e plats på digitaliseringsindexet, då är plats 41 rätt bra på informationssäkerhet men ligger du 2 3 4 5 på digitalisering och ligger så pass långt ner som vi gör här i Sverige på informationssäkerhet då, det här gapet, även om de inte är korrelerade de här 2 indexerna så är ju bekymret är ju gapet däremellan och som på din fråga på vilket sätt jag sysslar med digitalisering, det har det gör det är att konstatera att digitaliseringen har en baksida och det är den baksidan som vi har jobbar med.

Så jag jobbar ju inte medvetet med att förbättra digitaliseringen i samhället utan snarare att försöka mitigera de risker som uppstår tack vare att vi har en relativt långt gången digitalisering men att vi är dåliga på och skydda den, skyddar de digitala värdena.

Vilka utmaningar ser du med digitalisering?

det är just det är ju att vi för över mer och mer, både beroende och värde, i saker vi inte kan ta i, immateriella tillgångar och vi har inte hängt med när det gäller att skydda det här. Det finns ju så många enkla sätt att beskriva det, nu sitter vi hemma bägge två men, ta en människa på sin arbetsplats, om han eller hon kommer hem och någon har varit och stulit deras storbilds-TV då ser de det med en gång när de kommer hem för den är borta och den stod där i morse och stod inte där nu. Information kan du stjäla utan att någon har en aning om att det överhuvudtaget är på villovägar för den finns ju fortfarande kvar.

Så det finns enormt många utmaningar associerade med den här digitaliseringen, därmed inte sagt att vi inte ska digitalisera. För det är egentligen det enda sättet att driva effektiviteten i affärslivet framåt, men vi har låtit, och än så länge är vi ju fortfarande, digitalisering idag är ju väldigt mycket att det som fanns i pärmar finns nu i datorer så vi har ju inte fört över det så att det liksom innebär att vi förändrat våra arbetsrutiner och processer än, men det kommer väl, men vi har inte hunnit med och fundera på skyddet eftersom säkerhet är ju alltid betraktad som en kostnad det finns inget enkel sätt då härleda fördelarna till balans & resultaträkning och då är det svårt att hitta en styrelse och koncernledningsgrupper som tycker det är skoj att skicka iväg massor med pengar för att göra någonting som säkerhetshöjande.

Skulle du anse att personer i organisationerna har tillräcklig kompetens för att hantera digitaliseringen?

Nej alltså återigen, då måste ju skilja på det här eller ja definiera begreppet digitalisering. När det kommer till att pdf: a alla jävla dokument som har legat i pärmar och sorterat in dem i någon typ av filstruktur, för den kompetensen den finns nog. Men att vi att vi är fortfarande när vi pratar om digitalisering i huvudsak pratar om det och möjligtvis att flytta ut försäljningen vi gjorde i butiker till e-handelsplatser i stället, men det är ju väldigt simpel digitalisering och de delarna bedömer att det finns kompetens inom.

Däremot så har vi ju inte, det kan vara en kombination då av bristande kompetens och viss mån rädsla också, därför att för att låta då digitaliseringen och de möjligheter som en digitalisering kan innebära att låta det påverka och förändra våra kärnprocesser i verksamheten, affärsprocesser och andra verksamhetsprocesser, där är vi inte speciellt bra. Dels beror det nog på att vi har bristande kompetens men jag tror det också beror på att man känner sig lite att bekymrade för vad det här får för konsekvenser så det finns en viss rädsla eller ja man kan kalla det

feighet också om man vill. Kompetensbrist självklart och det har vi ju rent generellt i hela väldigt många sektorer i de här områdena men jag tror det är väldigt mycket att vi har inte riktigt förstått på vilket sätt vi kan använda, eller att vi kan ändra våra verksamhetsprocesser med hjälp av digitalisering. Då det var ju digitaliseringens biten när det kommer till att skydda det vi gör med digitaliseringen där är ju kompetensbristen ännu mycket större.

Om man tittar på digitalisering i samband med HR och människor, ser du någon särskild utmaning där?

Självklart det där är ju rätt intressant, när jag var på (företag) då kallar man ju inte HR utan då kallade man det HC, Human Capital, det är ju bara buzzwords, personalhantering är ju vad det är frågan om eller medarbetarhantering. I de här 90 procenten av immateriella tillgångar finns ju inte personal, och det blir ju väl väldigt snett. De flesta företag idag är ju är ju kunskapsföretag och då kan väl säga att, och då har man täckt upp de sista 10 procenten i det här totala värdet med personal, så att det är en väldigt, väldigt, viktig resurs och en väldigt värdefull resurs kanske ibland mycket värdefullare än vad man har för prislista eller för kundlista och då är ju alltså då är ju riskexponeringen ännu större när det kommer till att digitalisera HR delen av HR-processerna.

Det finns också tror jag, en överhängande risk att man avhumaniserar saker om man inte är jävligt duktig på digitaliseringen utav HR-delarna och det är inte bra. Speciellt när det är som idag och inom mina områden där jag är verksam inom, en enorm konkurrens om personal. Då har man inte råd att ha någon automatiserad process som inte funkar.

Sen har vi ju också ett en gigantisk riskexponering i och med att 2018 när GDPR blev svensk lag, så kan man ju konstatera att det mesta man hanterar inom HR, avseende personalinformation, är ju klassat som känslig information eller känsliga personuppgifter enligt gdpr med allt vad det innebär. Bara så här enkla saker som att när man skickar in en spontanansökan till ett företag så tror jag att 95 % av alla företag har inte en aning om vad man egentligen får inte får göra med så här spontant cv, hur ska man hantera den, de flesta sparar den säkert någon fil eller någon fil-struktur någonstans utifall att, helt omedveten om att man då bryter fett mot GDPR.

2) Informationssäkerhet

Hur arbetar du med informationssäkerhet i din roll?

Jättedåligt, verkligen, jag är inte ett dugg bättre än någon annan. Jag har hållit på med i över 20 år, jag har ju bara sysslat med sådant här men problemet med informationssäkerhet det är att det kolliderar med bekvämlighet och funktionalitet. Nej men är man då är extremt resultatintriktad som jag är, så är det oerhört frestsamt, eller det är inte bara frestande utan jag faller också de här frestelserna att ta the easy way out, för det går mycket fortare än att då hantera det på en korrekt informationssäkerhet sett.

Jag försöker, men jag är inte så jävla bra på det och problemet med informationssäkerhet det är att man önskar ju att det fanns någon gordisk knut som man med ett alexanderhugg kunde öppna upp genom att köpa någon pryl men så är det ju inte utan informationssäkerhet är ju primärt, beteenden, processer, rutiner och policys. Så det är jobbigt att vara informationsäker, även för någon som vet vikten av det som jag.

Hur tror du man ska jobba för att skapa medvetenhet kring informationssäkerhet?

Utbilda, utbilda, utbilda, utbilda, utbilda, och utbilda igen. Jag höll ett föredrag om företagshemligheter, jag vet inte vad det kan ha varit 130-140 bolagsjurister och det var ju väldigt uppenbart att när man kommer in på de här, nu var det ju fokus på företagshemligheter, men då är ju informationssäkerhet ett sätt att skydda företagshemligheter, och det var väldigt uppenbart att de helst skulle vilja att jag sa "köp den här lådan så kommer allting att lösa sig" men det är ju inte så, utan det mesta är inte teknik, det är första man måste göra och som kanske det jobbigaste och tråkigaste det är att ha ett bra grepp om vad det är man gör på företaget att man har beskrivit alla sina processer och vet vad det är man gör.

Steg 2 det är att identifiera all information som man hanterar och klassificerar den som man vet vad som är öppet eller vad som var ska företagsinternt eller måste vara jättehemligt. Sen så måste man ju se till att man inte kommer åt mer information än det man behöver för sin roll eller författning och det är också jättekrångligt, någon måste sitta och definiera upp det, är man säljare med ansvar för Småland då är det den här typen av information som man får komma åt och ingen annan, och sen så måste man då ta fram policys som säger vad man får och inte får göra och vad man ska och inte ska göra och sen måste man utbilda, utbilda, utbilda och utbilda, och kontrollera, och utbilda, så vi i huvudsak så är informationssäkerhet det är ju skittråkigt, det är jobbigt och tråkigt, och det är mycket enklare att säga att ja men vi skjuter till 5 miljoner och köper några brandväggar men det är ju helt värdelöst.

HR har eller alltså personalfunktionen och en enormt viktig del i informationssäkerhet, inte som teknikbärare utan liksom som kulturbärare. Jag har jobbat väldigt mycket mot både militära och polisiära underrättelser och säkerhetstjänster, då har de ju ändå mäktiga fiender men alla landar i samma definition och det är att över tiden så är insidern alltid det största hotet alltså det är liksom personalen, som medvetet eller omedvetet, gör så att man får informationsförluster, så det visar ju på behovet att både kontrollera sina medarbetare och utbilda dem.

Vad ser du för utmaningar när det kommer till informationssäkerhet?

Ett, om jag tittar från mitt från min horisont eller från leverantörssidan, så är ju en utmaning det är ju att vi aldrig har varit speciellt bra på att kunna visa för kunden, eller den presumtiva kunden, vad det finns för positiv nytta utav informationssäkerhet. Vi har alltid ett ganska negativt sätt att sälja in våra saker, det är liksom om du inte anlitar oss eller inte gör det här då kan något jättehemskt hända dig, det är ju inte positivt. Medan det finns andra, från marknadsföringsföretag och andra, de kommer ju till en kund och säger vi kan hjälpa dig att tjäna ännu mer pengar, så från vår industri så är ju det ett av bekymren, att vi har ganska tråkiga säljbudskap, du vet att livet är kort du kommer snart att dö och då kommer all information eller skillnad, så nu ska du anlita oss. Det är sjunde inseglet tråkigt.

När det kommer då till den andra sidan, alltså vad det finns för generellt bekymmer, så dels så det här har ju ändrats när jag startade (företag) år 2000, då var jag ju på för att vår huvudsakliga uppgift det var ju egentligen att visionera och missionera och försöka förklara vad informationssäkerhet var överhuvudtaget och då vi sålde ju då väldigt mycket mot polis, Säpo och militära underrättelsetjänsten och liknande därför dom visste behovet men banker och andra var ganska ointresserade. Så att jag har ju spenderat väldigt mycket utav de första 10–15 åren med någon typ av folkbildning, eller försöka få ut det här budskapet. Idag har vi inte det problemet, det du kan ju få på text tv, gå in på vilken nyhetssajt som helst så hittar du minst ett par gånger i veckan i alla fall, nyheter om informationsförluster och breaches och liknande så medvetenheten som länge, länge, länge, var det stora problemet den har ju blivit bättre i alla fall, den är inte jättebra, men det har blivit bättre, men den har ju inte blivit så bra så att man är beredd att ändra sina egna beteenden för att leva säkert.

Jag menar, det gör ju inte jag heller så jag ska inte klanka ner, så utbildning, medvetenhet plus att vi har alldeles för få resurser som har kompetens inom de här områdena.

Upplever du att det finns en risk att obehöriga får tillgång till känsliga data när man digitaliserar?

Absolut, det var det fanns det redan innan man digitaliserade och nu när vi digitaliserar då ökar vi ju bara riskexponeringen och vi skapar fler... så här, i vår bransch så pratar man ju om angreppssektorer och i och med att vi digitaliserar mer och mer så ökar vi ju liksom ytan, vår sårbara yta mot omvärlden, så att det är för vekt att bara säga ja, det gör det, utan det gör det exponentiellt, digitaliseringen ökar risken och utsattheten exponentiellt och det är ju obra kan jag ju säga.

Ser du några andra risker med molntjänster jämfört med annan typ av datalagring?

Ja det finns någon, men när Cloud blev ett Buzz Word för ett antal år sedan, då såg jag en jävligt rolig meme, det var bild på, har du sett filmen matrix? Då han Laurence Fishburne, som spelar den här coola snubben, då är det en bild på honom med sina coola glasögon och så står det bara "what if I said to you the cloud is just somebody elses computer", för det är ju det, det är frågan om, det är det som är den stora riskexponeringen med molntjänster, det betyder nämligen att du bara lägger ut det här på någon annans utrustning, som du hoppas och tror, eller det här är intressant, molnen är väldigt bra att exemplifiera det jag försökte kanske otydligt ge uttryck för tidigare nämligen att vår lathet och strävan efter enkelhet och slippa ifrån bekymmer, det gör att vi är villiga att sätta oss i väldigt riskutsatta positioner för Cloud är en sån, det känns ju supermysigt att slippa köpa datorer och servrar och anställda IT personal som ska se till att allt det här funkar och förutom att vara uppe i molnet. men det är håll i huvudet och nu har ju GDPR med all önskvärd tydlighet, alltså jag vet inte hur mycket ni har läst inne på schrem 2, det visar ju med all önskvärd tydlighet de utmaningar som man har och eftersom USA är fortfarande alltså, inte ses som en safe harbour för personuppgifter, du har ingen aning om var din information landar när du laddar upp till molnet.

Så säger man ja men vi måste lita på Google, och vi måste ju lita på Amazon, och Microsoft med Azure, men nej det kan man inte göra man kan inte lita på amerikanska bolag eftersom alla de omfattas av patriot act från någon gång 80 där de då är tvungna att släppa ut information till amerikanska underrättelseorganisationen ifall de kräver det och sen har ju amerikanerna, känner du till det som heter Cloud Act? det är ju det är ju faktiskt på gränsen till väldigt roligt därför Cloud Act står för The Clarifying Lawful Overseas Use of Data Act, så det har ju egentligen ingenting med cloud att göra men det var det säger det är att amerikanska myndigheter har också rätt att kräva in information från amerikanska företags servrar även om de står i andra länder. Så Microsoft försökte då lägga sin molnserver för Azure på Irland, men där hade man ju ett moln för något år sedan

där amerikanska myndigheter tvingade Microsoft att lämna ut information på de servrar som stod på Irland, så moln, nej, inget bra.

Hur påverkade införandet av GDPR ditt sätt att arbeta?

Inte, jo okej, det är 2 olika saker, i mitt sätt att arbeta om du ser när jag leder och bygger företag och så... 1997 eller någonting ja, kom EU:s dataskyddsdirektiv och ett direktiv du får ju varje medlemsland massera in hur man vill i lagstiftningen och det gjorde vi ju genom PUL, personuppgiftslagen... Men, 2018 så kommer ju då dataskyddsförordningen och den får man ju inte pilla på utan den måste man lyfta in as is, i sin lagstiftning vilket vi och alla andra länder gjorde. Men vad GDPR inneburit är ju att har hamnat på agendan och man har börjat sakta men säkert, alltså då var jag fortfarande kvar på (företag) och jag har gjort kanske 40 eller 50 stora gap-analyser mot företag organisationer kring GDPR och jag åkt runt och liksom hållit föredrag och missionerat över hela landet, det har tagit efter lång tid, men nu börjar faktiskt polletten trillar ner, inte minst eftersom vår tillsynsmyndighet har ju börjat utfärda vitesbelopp till och med till myndighetsvärlden, alltså så det är ju liksom det är ju regioner som får betala 7 miljoner för att man inte har skött sig och så det här kommer ju mer och mer.

Vad det betyder rent generellt för mig och för vår bransch, förutom att det är en typ av tjänster som vi nu helt plötsligt kan börja leverera, så är det att medvetenheten om att information har på något sätt ett värde har ju ökat väldigt mycket, även om det i första hand inom GDPR är för att man är rädd för att få sanktioner mot sig. Jag tycker GDPR är bra, för när man vet vad man kan göra med personuppgifter och den digitaliseringen som vi trots allt har idag vad den innebär, då är det väldigt bra att man försöker sätta stopp på det här på något sätt. Det är bara se Cambridge Analytica hur man med all sannolikhet, ganska omfattande, påverkan det valet både i USA och brexit valet i England. Så jag är, inte bara för att jag kan sälja tjänster inom området, men jag tycker det är väldigt viktigt att man har den här personliga integriteten så att man inte riskerar, ja, har påverkat jättemycket. Det är ju på samtals, det är på agendan, företagen pratar om det för de vill inte, alltså att ta 7 miljoner eller 15 miljoner från sin resultaträkning det är inte någon som vill göra det så GDPR är, det är väldigt bra.

Nu har vi pratat om digitalisering, digitalisering i samband med HR och informationssäkerhet, finns det någonting som du känner är en viktig input om man korrelerar de 3 områdena?

Ja, jag kan ta några funderingar. När det kommer till digitalisering utav personalprocesserna så tror jag att risken är kombinerad både finns det en exponeringsrisk alltså det som de traditionella informationssäkerhetsriskerna som är integritet, konfidentialitet och så kombinerat med att man tappar lite grann här fingertoppskänslan som krävs för att hantera materia, personal och från resurser. Det var min grundidé när jag när jag startade mitt första bolag, det gjorde det egentligen inte för jag var superintresserad av informationssäkerhet, jag gjorde det därför att jag ville testa mina egna idéer och funderingar på hur man skulle skapa företagskultur och så, och där finns ju en risk för att Hr, nu ska jag dra alla HR över en kant, men HR vill ju gärna dela in saker och ting i fack, det bli mer lätthanterligt.

När jag jobbade på (namn) tillexempel då var det ju så här, jag hade en jättebra medarbetare som hade fått skulle få högre lön på HP, än på (namn), så gick jag till min HR och sa att nu tänker jag hur höja hans lön med fyratusen kronor och då sa ju min hr, nej men han är ju en 43 7 streck B och deras lönespann det här så han, så han har redan en sån lön, men han slutar om man inte får, ja men då får du anställa en ny 43 7 streck B, men det är inte så det funkar och digitalisering finns det ju en risk att det blir ännu mer opersonligt, för HR eller personal hanteringen och när det kommer då just framförallt till branscher som har ett bekymmer att rekrytera och säkerställa tillgången på kompetenta människor då tror jag att det är en större risk, HR-digitalisering, än själva säkerhetsrisken, att det blir för mekaniserat och att man tappar folk på grund av det, annars så är det ju ja, det är väl att det är det är det är alltid krångligt om man ska göra någonting säkerhetsmässigt, det är alltid mycket krångligare, eller alltid mycket lägre funktionalitet än om du skiter i säkerhet helt och hållet, så att mänsklighetens inneboende ryggradsreflex det är ju att ta the easy way out.

Referenser

- Aberge, T., Bellevrat, E., Benne, S., Berly, T., Kubecek, V., Law, G.Y., o.a. (2017). Digitalisation and Energy. International Energy Agency
- Alotaibi, M.J., Furnell, S. & Clarke, N. (2019). A framework for reporting and dealing with end-user security policy compliance. *Information & Computer Security*.
- Alvehus, J. (2016). Skriva uppsats med kvalitativ metod: en handbok. Stockholm. Liber AB.
- Andress, J. (2014). The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Syngress.
- Ahnlund, A. (2018). Så tar HR nästa steg i sin digitalisering. HRbloggen.se Tillgänglig: <https://hrbloggen.se/2018/04/hr-nasta-steg-digitalisering.html> [Hämtad: 2022-05-16]
- Arbetsmiljöverket (2018). Gränslöst arbete. Rapport 2018:1 Stockholm. https://www.av.se/globalassets/filer/publikationer/rapporter/granslost-arbete-en-forskarantologi-om-arbetsmiljoutmaningar-i-anknytning-till-ett-granslost-arbetsliv_rap2018_1.pdf [Hämtad: 2022-05-16]
- Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, vol. 53, no.4
- BBC. (2020). Coronavirus confirmed as pandemic by World Health Organization, 11 Mars. Tillgänglig på: <https://www.bbc.com/news/world-51839944> [Hämtad: 2022-05-16]
- Bryman, A. (2018). Samhällsvetenskapliga metoder. 3. uppl., Stockholm: Liber AB
- Börjesson, F. (2020). Effektiv Digitalisering, en överlevnadsbok för verksamheten. Stockholm: Books on Demand. s.10-11
- Dalen, Monica. (2015) *Intervju som metod*. 2 uppl. Falkenberg: Gleerups Utbildning AB.
- Denscome, M. (2009) *Foskningshandboken*. Lund: Studentlitteratur AB.
- Europakommissionen. (2020). Telework in the EU before and after the COVID-19: where we were, where we head to. Tillgänglig på: https://ec.europa.eu/jrc/sites/jrcsh/files/jrc120945_policy_brief_-_covid_and_telework_final.pdf [Hämtad: 2022-05-16]
- Evans, A., Martin, K., Poatsy, M.A, *Technology in Action. Complete. 16th edition*. (2021) Pearson Education, London.
- Findikli, M. A., & Bayarçelikb, E. B. (2015). *Exploring the outcomes of Electronic Human Resource Management (E-HRM)*. https://ac.els-cdn.com/S1877042815052453/1-s2.0-S1877042815052453-main.pdf?_tid=ced2fd01-0e96-4372-84af-e15c3f7367f0&acdnat=1520947729_e198d7f1750859d4bc4e45d12764a4de [Hämtad: 2022-05-16]
- Forsström, L. (2021). Föreläsning: HR-digitalisering och dess möjligheter. Akademikerförbundet SSR. <https://akademssr.se/post/forelasning-hr-digitalisering-och-dess-mojligheter>
- Jacobsen, D. I. (2002). Vad, hur och varför: om metodval i företagsekonomi och andra samhällsvetenskapliga ämnen, Lund: Studentlitteratur
- Jesuthasan, R. (2017). HR's new role: rethinking and enabling digital engagement. *Strategic HR Review*. 16(2).
- Kraemer, S. & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied ergonomics*, vol. 38, no. 2
- KPMG (2020) The future of HR 2020: which path are you taking. Tillgänglig: <https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/11/future-of-hr-2020.pdf> [Hämtad: 2022-05-16]
- Lengnick-Hall, M., & Moritz, S. (2003). *The Impact of e-HR on the Human Resource Management Function*. *Journal of Labor Research*, 24(3), 365-379. Tillgänglig: <https://link.springer.com/content/pdf/10.1007%2Fs12122-003-1001-6.pdf> [Hämtad: 2022-05-16]
- Lillkrona, M. (2022). Så kan HR digitaliseras och följa GDPR. Knowit. Tillgänglig: <https://blogg.knowit.se/cybersakerhet-och-juridik/sa-kan-hr-digitaliseras-och-folja-gdpr> [Hämtad: 2022-05-16]
- Lind, L.(2020). *Hur HR-rollen har förändrats - och fortsätter att formas*. Talentech. <https://blog.talentech.com/sv/hur-hr-rollen-har-forandrats-och-fortsatter-att-formas>
- Liu, S., Chan, F. T., Yang, J. & Niu, B. (2018). Understanding the effect of cloud computing on organizational agility: An empirical examination, *International Journal of Information Management*, vol. 43
- MSB (2021) Informationssäkerhet, cybersäkerhet och säkra kommunikationer. Tillgänglig: <https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/cyberhot/> [Hämtad: 2022-05-16]
- Möller. P.F. Dietmar (2020). Introduction to Cybersecurity. In: *Cybersecurity in Digital Transformation*. SpringerBriefs on Cyber Security Systems and Networks. Springer, Cham. Available: https://doi-org.ludwig.lub.lu.se/10.1007/978-3-030-60570-4_2 [Hämtad: 2022-05-16]
- Oates, B. J. (2006). Researching information systems and computing, London: SAGE.

- Simpleyer. (2020). Det brådskar att digitalisera HR. <https://www.simpleyer.se/artiklar/det-bradskar-att-digitalisera-hr/> [Hämtad: 2022-05-16]
- Parviainen, P., Kääriäinen, J., Tihinen, M., & Teppola, S., (2017). Tackling the digitalization challenge: how to benefit from digitalization in practice. *International Journal Of Information Systems And Project Management*, Vol 05, Issue 01, Pp 63-77, (01), 63.
- Popović, K. & Hocenski, Ž. (2010). Cloud computing security issues and challenges, *The 33rd international convention MIPRO*
- Rienecker, L. & Stray Jörgensen, P. (2014). Att skriva en bra uppsats. 4th ed., Malmö: Liber
- Rizwan, S. & Zubair, M. (2019). Basic Security Challenges in Cloud Computing, *2019 4th International Conference on Emerging Trends in Engineering, Sciences and Technology (ICEEST)*
- Siponen, M. (2000). *A conceptual foundation for organizational information security awareness*. Information Management & Computer Security. Vol.8. No.1
- Skrodelis, H.K., Strebko, J. & Romanovs, A. (2020). October. The Information System Security Governance Tasks in Small and Medium Enterprises. In *2020 61st International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)*. pp. 1-4. IEEE
- Som, A. (2008). *Innovative human resource management and corporate performance in the context of economic liberalization in India*. The International Journal of Human Resource Management, 19(7), 1278-1297
- Statens Offentliga Utredningar, SOU 2015:91 - tillgänglig: <https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2015/12/sou-201591/> [Hämtad: 2022-05-16]
- Statens Offentliga Utredningar, SOU 2016:89, Tillgänglig: <https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2016/12/sou-201689/> [Hämtad: 2022-05-16]
- Stone, D. L., Deadrick, D. L., Lukaszewski, K. M., & Johnson, R. (2015). The influence of technology on the future of human resource management. *Human Resource Management Review*, 25(2)
- Tillväxtverket (2020) Tillgänglig: <https://tillvaxtverket.se/download/18.3011b666175e07e3a84170ce/1606142312649/Informationssakerhet%20rapport%20reviderad.pdf> [Hämtad: 2022-05-16]
- Townsend, A., & Bennett, J. (2003). Privacy, technology, and conflict: emerging issues and action in workplace privacy. *Journal of Labor Research*, 24
- Trost, A. (2020). *Human Resources Strategies - Balancing Stability and Agility in Times of Digitalization*. Springer. Cham. Tillgänglig: <https://doi.org/10.1007/978-3-030-30592-5> [Hämtad: 2022-05-16]
- Ulrich, D. and Dulebohn, J.H., (2015). Are we there yet? What's next for HR?. *Human Resource Management Review*, 25(2)
- Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, 18
- Whitman, M., & Mattord, H. (2011). *Principles of Information Security*. 4th ed. Boston: Thomson Course Technology
- Wood, C.C. & Banks Jr, W.W., (1993). Human error: an overlooked but significant information security problem. *Computers & Security*, vol. 12, no. 1
- Wylder, J., (2003). *Strategic Information Security*. United States: CRC Press.
- Wikander, S. (2020) *Digitaisering: Experterna om digitala HR-processer, trender och verktyg inför 2021*. Scandinavian Recruitment Intelligence Tillgänglig: <https://sri.se/blogg/digitalisering-hr-processer-verktyg-2021/> [Hämtad: 2022-05-16]
- Zissis, D. & Lekkas, D. (2012). Addressing cloud computing security issues, *Future Generation computer systems*, vol. 28, no. 3
- Ågren, D. (2019) *Digitalisera HR-processer - skapa en medveten kultur*. Tillgänglig: <https://www.wiseconsulting.se/insikter/digitalisera-hr-processer-skapa-en-medveten-kultur/> [Hämtad: 2022-05-16]