LUNDS UNIVERSITET
Ekonomihögskolan

Företags syn på anställdas dator- och Internetanvändning

- *När är du anställd och när är du privat?*

Kandidatuppsats, 15 högskolepoäng, SYSK02/INFK11 i informatik

Framlagd: Maj, 2014

Författare: Jan Gadimzadeh & Ashkan Moghtaderi

Handledare: Anders Svensson

Examinatorer: Markus Lahtinen & Paul Pierce

Titel: Företags syn på anställdas dator- och Internetanvändning – När är du anställd och när är du privat?

Författare: Jan Gadimzadeh
Ashkan Moghtaderi

Utgivare: Institutionen för Informatik

Handledare: Anders Svensson

Examinator: Markus Lahtinen
Paul Pierce

Slutseminarium 2014, Maj

Uppsatstyp: Kandidatuppsats

Nyckelord: Internetpolicy, BYOD, sociala medier, dator- och Internetanvändning, övervakning, privat

Abstrakt

Den kraftiga utvecklingen av Internet, sociala medier och BYOD har påverkat företags syn på anställdas privata och yrkesverksamma dator- och Internetanvändning. Företag måste idag anpassa verksamheten för att på bästa sätt utnyttja de positiva aspekterna, men samtidigt också undvika de risker och hot som kan skapas. Syftet med studien är att belysa hur företag påverkas av anställdas dator- och Internetanvändning, både på arbetsplatsen och på fritiden.

För att besvara detta har semistrukturerade telefonintervjuer och besöksintervjuer genomförts med två större och två mindre företag. Genom analysen av dessa intervjuer framgår det att större och mindre företag inte påverkas på samma sätt.

Undersökningen visar att större företag är mer försiktiga och medvetna i frågan, medan mindre företag är mer positivt inställda och inte känner ett behov av att anpassa verksamheten efter anställdas privata och yrkesverksamma dator- och Internetanvändning.

Innehållsförteckning

1 Inledning

Det första kapitlet behandlar bakgrunden till vårt ämnesval samt en problemformulering inom området. Utifrån problemdefinitionen har vi formulerat vår forskningsfråga, förklarat syftet med uppsatsen samt de avgränsningar som har gjorts. Detta kapitel syftar till att ge läsaren en större förståelse och bakgrund till vårt ämnesval.

1.1 Bakgrund

Informationsteknologins (IT) framskjutna position i dagens samhälle innebär en mängd olika fördelar för både privatpersoner och företag, såsom Internet, e-post, mobiltelefoner och mycket mer. Detta är inget undantag för Sverige då 88% av svenskarna har tillgång till och använder sig av Internet regelbundet, vilket gör att Sverige har världens högsta andel Internetanvändare i förhållande till den totala befolkningen (Findahl, 2011). Detta har inneburit en stor förändring för svenska företag som tidigare enbart använt Internet som ett medel för kommunikation och e-post. Idag är Internet ett väsentligt redskap för att företag ska kunna vara konkurrenskraftiga och ett nödvändigt arbetsverktyg i det dagliga arbetet, men det innebär också en hel del eget ansvar.

Det är ingen nyhet att det finns anställda som använder tillgången till Internet för privata ändamål, till exempel genom att privatsurfa på andra hemsidor under arbetstid. Enligt Simmers & Bosnian (2002) kan detta innebära att företag tappar i effektivitet och dessutom vara en säkerhetsrisk ur flera perspektiv. Däremot har problematiken med anställdas dator- och Internetanvändning blivit mer komplex än så. Idag är privatpersoner mer aktiva på sociala medier än företagen och föredrar dessutom att använda sin egna tekniska utrustning på arbetsplatsen (Stepstone, 2013). Detta kan medföra risker och hot som är ett resultat av gränsdragningsproblematiken mellan anställdas yttrandefrihet och lojalitetsplikt, men även hur regler och riktlinjer bör förhållas i arbetslivet gentemot privatlivet.

Det blir allt vanligare att publicera studier och artiklar om de effekter och konskevenser som skapas av företags närvaro i sociala medier samt den nya BYOD-trenden (Bring Your Own Device), men resultaten kan se annorlunda ut. Det börjar till och med bli vanligt att företag kontrollerar sina anställdas dator- och Internetanvändning för att på bästa sätt undvika den problematik som kan uppstå. Allt detta skapar en verklighet som kan vara bekymrande för båda sidorna ur flera perspektiv och den verkligheten kommer ligga i fokus i den här uppsatsen.

1.2 Problemformulering

Den kraftiga utvecklingen av Internet, sociala medier och BYOD har påverkat och förändrat företags syn på anställdas dator- och Internetanvändning, både på arbetsplatsen och på fritiden. Privatpersoners användning av sociala medier har ökat markant de senaste åren och därför har det blivit populärt att även företag närvarar i dessa nätverk. I takt med att smartphones och surfplattor också blivit en del av vardagen för privatpersoner, har önskemålen ökat på att släppa in dessa på arbetsplatsen. Denna utveckling har förändrat anställdas dator- och Internetanvändning och gynnat både företagen och dess anställda på flera sätt – företag genom att åstadkomma affärsmål och anställda genom att mer effektivt utföra sina arbetsuppgifter.

Däremot har denna utveckling också inneburit en hel del frågetecken och komplicerade beslut som företagen måste tackla. Vi anser att mycket tyder på att företag påverkas av denna utvekling och måste därför anpassa verksamheten för att på bästa sätt utnyttja de positiva aspekterna, men samtidigt också undvika de risker och hot som kan skapas. Vi vill därför undersöka på vilket sätt företag påverkas av anställdas privata och yrkesverksamma dator- och Internetanvändning. Med ”dator- och Internetanvändning” menar vi surfvanor, användning av sociala medier och teknisk utrustning samt övriga Internetaktiviteter.

1.3 Forskningsfråga

Vi har formulerat följande forskningsfråga utifrån problemformuleringen:

- Hur påverkas företag av anställdas privata och yrkesverksamma dator-och Internetanvändning?

1.4 Syfte

Syftet med vår uppsats är att belysa hur företag påverkas av anställdas privata och yrkesverksamma dator- och Internetanvändning. Genom att identifiera de effekter som skapas av anställdas användning av sociala medier och fenomenet BYOD hoppas vi kunna belysa på vilket sätt företag påverkas av denna utveckling.

1.5 Avgränsning

Avgränsningar har gjorts till företag som är närvarande i sociala medier eftersom en stor del av vår studie kommer behandla anställdas vanor på de plattformerna. Vi har även avgränsat oss till företag på den svenska marknaden av praktiska skäl, men även på grund av att Sverige ligger i framkant när det gäller privat användning av Internet-teknologi (Findahl 2011).

1.6 Läsanvisning

Vår uppsats är uppbyggd och strukturerad kring följande kapitel:

- *Kapitel 1: Val av ämne, problemdiskussion och syfte* – Kapitlet behandlar bakgrunden till vårt ämnesval samt en problemformulering inom området. Utifrån problemdefinitionen har vi formulerat vår frågeställning, förklarat syftet med uppsatsen samt de avgränsningar som har gjorts.

- *Kapitel 2: Litteraturgenomgång* – Litteraturgenomgången är en studie av tidigare publicerad litteratur och artiklar. I litteraturgenomgången presenterar vi teorier som är viktiga för att skapa djupare kunskap i ämnet.

- *Kapitel 3: Metodval och metoddiskussion* – Här redogör vi och argumenterar för vilka metoder vi valt och varför de uppfyller syftet med vår uppsats. Vi presenterar även en modell över vårt tillvägagångsätt under studien.

- *Kapitel 4: Redovisning av kvalitativ undersökning samt analys av insamlat material* – I detta kapitel redovisas resultatet av vår kvalitativa undersökning samt en grundläggande analys.

- *Kapitel 5: Diskussion* – I detta kapitel kommer de resultat som erhölls genom föregående kapitel att diskuteras närmare med stöd av uppsatsens teoretiska ramverk.

- *Kapitel 6: Slutsatser* – I uppsatsens avslutande kapitel kommer vi redovisa våra slutsatser.

2 Litteraturgenomgång

Litteraturgenomgången är en studie av tidigare publicerad litteratur och artiklar och syftar till att skapa djupare kunskap i ämnet. Vi kommer presentera teorier som hjälper läsaren att förstå vårt ämnesområde.

2.1 Kontroll och integritet

Vi kommer nedan presentera hur personuppgifter regleras i arbetslivet för att kontrollera och övervaka anställdas dator- och Internetanvändning. Vi kommer även förklara Internetpolicy som är en central del av uppsatsen.

2.1.1 Övervakning i arbetslivet

Det blir allt vanligare att svenska företag kontrollerar anställdas dator- och Internetanvändning, framförallt större företag. Sådana kontroller görs främst för att säkerställa att personalen följer de regler och riktlinjer som arbetsgivaren har utformat. Arbetsgivaren måste dock vara försiktig i samband med sådan övervakning. Lagöverträdelser i samband med övervakning av anställda kan resultera i allvarliga sanktioner och kan vara förödande för företaget. (IT & Telekomföretagen, 2013)

Innan arbetsgivaren kontrollerar anställdas dator- och Internetanvändning måste personalen blivit informerade om ändamålet med övervakningen. Därför borde arbetsgivaren först upprätta en Internetpolicy där anställdas rätt att använda Internet, e-post, företagets utrustning och liknande regleras. Internetpolicyn borde även innehålla reglering av personuppgifter eftersom övervakning i arbetlivet innebär att PuL (personuppgiftslagen) blir tillämplig. (IT & Telekomföretagen, 2013)

Enligt Delphi (2013) anses intrånget i den personliga integriteten vara mer allvarlig vad gäller övervakning av anställdas privata enheter på arbetsplatsen. Användandet av anställdas egna tekniska utrustning på arbetsplatsen kallas för BYOD vilket kommer diskuteras senare i uppsatsen. Om arbetsgivaren får tillgång till den anställdes privata enheter utan samtycke kan detta resultera i dataintrång.

2.1.2 Internetpolicy

Internetpolicy är ett centralt begrepp i vår uppsats och måste därför studeras närmare. I vår empiriska undersökning är vi intresserade av att veta om företag har en Internetpolicy för anställdas dator-och Internetanvändning. Vi behöver därför studera begreppet för att kunna formulera mer utförligare frågor till företagen samt förstå innebörden av begreppet bättre.

En Internetpolicy är riktlinjer och regler för anställdas dator-och Internetanvändning som utformas av företagets arbetsgivare. En sådan policy syftar till att alla på arbetsplatsen ska vara medvetna om vilka regler som finns och dessutom att reglerna följs. Därför är det viktigt att kommunicera policyn med företagets anställda och skapa rutiner för hur information om reglerna ska nå alla som anställts. Innehållet i en Internetpolicy måste utformas med

utgångspunkt i den verksamhet som arbetsgivaren bedriver. Det är arbetsgivarens ansvar att avgöra vilka förutsättningar och vilket skyddsbehov som finns samt kontrollera att de regler som fastställts i policyn följs. (IT & Telekomföretagen, 2013)

Nedan följer exempel på vilka typer av regleringar som kan förekomma i en Internetpolicy:

- Vilken typ av användning av Internet är tillåten respektive otillåten?
- Är det tillåtet att delta i chat-sidor eller diskussionsforum?
- Är det tillåtet att för privata syften besöka webbplatser med extrempolitiskt eller pornografiskt innehåll?
- Allt som berör kontroll av anställdas dator-och Internetanvändning samt säkerhetsfrågor. (IT & Telekomföretagen, 2013)

Enligt Welebir & Kleiner (2005) ska en Internetpolicy alltid ha ett kapitel som berör säkerhetsaspekterna av anställdas dator-och Internetanvändning. Detta kapitel är nödvändigt eftersom arbetsgivaren måste betona vilka konsekvenser som kan drabba företaget om information läcker ut eller om datorer drabbas av virus. De flesta anställda är medvetna om att Internet är fullt av hemsidor med säkerhetsrisker, men arbetsgivaren måste trots detta förklura hur exempelvis virus kan spridas via e-post och liknande. (Welebir & Kleiner, 2005)

En Internetpolicy bör innehålla ett kapitel om övervakning och filtrering. Anställda har lagsskyddad rättighet att veta om deras aktiviteter på Internet är övervakade av arbetsgivaren och hur länge sådan information sparas. Filtrering är också ett nödvändigt verktyg eftersom företaget visar vilka typer av hemsidor som verksamheten inte står bakom. Detta kan exempelvis vara webbplatser med extrempolitiskt innehåll. (Welebir & Kleiner, 2005)

När arbetsgivaren har framställt en färdig policy måste denna skickas till företagets anställda. Det vanligaste är att alla anställda får en kopia som de måste läsa igenom och skriva under. Det måste framgå i policyn varför företaget behöver en policy för anställdas dator- och Internetanvändning, så båda parter kan sammarbeta i frågan vilket gynnar hela verksamheten. (Welebir & Kleiner, 2005)

2.1.3 Tidigare studie om Internetpolicy & övervakning

En omfattande studie från Datainspektionen (2005) undersökte kontroll av anställdas Internet- och e-postanvändning. Undersökningen inleddes med att 103 slumpvis valda företag och myndigheter skriftligen i en enkät fick besvara frågor om anställdas Internet- och e-postanvändning.

Resultaten av studien visar att de flesta arbetsgivare har någon form av dokumenterad IT-policy som mer eller mindre reglerade de anställdas rätt att använda Internet och e-post. Av de 103 arbetsgivarna uppgav 91 att de hade regler för den anställdes Internetanvändning och i 84 fall fanns dessa regler dokumenterade. (Datainspektionen, 2005)

I resultatet framgick det även att 44 av arbetsgivarna utförde någon form av kontroll av anställdas Internetanvändning. Däremot svarade 19 att de saknade regler och riktlinjer för hur en sådan kontroll skulle ske. (Datainspektionen, 2005)

Resultatet för anställdas e-postanvändning liknar Internetanvändningen. Där uppgav 103 arbetsgivare att de har regler för den anställdas e-postanvändning, och i 78 fall fanns dessa dokumenterade. (Datainspektionen, 2005)

2.1.4 Personlig integritet

En problematik som måste beaktas vid ett ämnesval av vår typ är risken för kränkning av den personliga integriteten. Detta gäller inte bara för övervakning av anställdas dator-och Internetanvändning, utan personlig integritet är ett central begrepp som är kopplat till övervakning av människor, oavsett om teknik är inblandat. Därför anser vi att personlig integritet är relevant för vår studie och nedan följer en beskrivning av begreppet.

Enligt Bylund (2013) finns det inget kort och entydligt svar på vad personlig integritet är för något. Han menar att det för många handlar om möjligheten, eller rentav rätten, att kontrollera spridning och användning av personlig information. Bylund (2013) betonar att det inte är lätt att definiera begreppet och att personlig integritet betyder olika för många beroende på vilket perspektiv man har.

Något som kan fastställas är att personlig integritet berör sekretessfrågor i PuL och denna lag kommer att beskrivas nedan.

2.1.5 Personuppgiftslagen

PuL är relevant för vår studie eftersom lagen skall skydda den personliga integriteten vid databehandling av personuppgifter (Junesjö, 2000). Enligt Justitiedepartementet (1998) så är syftet med lagen att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter.

PuL är aktuellt vid flera situationer som berör anställdas dator- och Internetanvändning. Ett exempel på tillämpningsområde för PuL finns vid övervakning av anställdas e-post och surfvanor. Dessa områden kan uppfattas som integritetskänsliga och därför blir PuL aktuellt. Ett annat exempel då PuL är aktuellt finns vid när- och frånvaroregistrering samt personaladministrativa områden. (Datainspektionen, 2003)

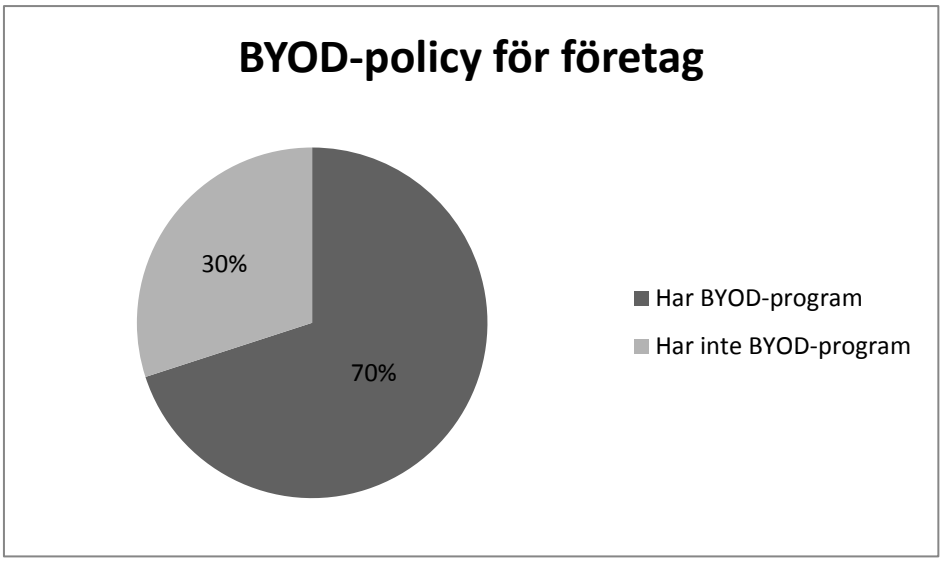
Enligt Justitiedepartementet (1998) kan straffet för brott mot PuL bli böter eller fängelse i högst sex månader. Fängelsetiden kan utökas till två år om brottet anses vara allvarligt nog. Om någons personuppgifter behandlas i strid mot PuL kan detta resultera i skadestånd för den individen på grund av kränkning av den personliga integriteten.

2.2 BYOD – Bring Your Own Device

I samband med vårt ämnesval är det viktigt att förstå en trend som har ökat markant i takt med framförallt smartphoneutvecklingen de senaste åren. BYOD avser en företagspolicy som tillåter anställda att ta med sig sin egna tekniska utrustning till arbetsplatsen, som exempelvis smartphones, surfplattor och bärbara datorer. Begreppet är relativt nytt och är ett resultat av att användare önskade att kunna interagera med andra användare via olika typer av kommunikationsmedel oavsett vilken plats de befinner sig på. Därför ersattes begreppet BYOC (Bring Your Own Computer) som refererar till anställdas möjlighet att ta med sig datorn, med det mer flexibla och moderna konceptet BYOD. (BBC, 2012; Cisco, 2013)

Det traditionsenliga arbetssättet inom företag har länge varit att anställda använder sig av företagsägda enheter. Införandet av en BYOD-policy syftar till att anställda istället använder sig av egna enheter för att skicka och dela data. Den utrustning som anställda väljer att tag med sig till arbetsplatsen ansluts då till företagets nätverk och detta kan medföra konsekvenser för verksamheten, vilket senare kommer förklaras utförligare. (VMware, 2013)

Idag är det vanligt att svenska företag tillämpar en BYOD-policy och trenden blir allt större och vanligare, men medför också risker och hot för både företagen och dess anställda (CIO Sweden, 2013). Enligt en global undersökning från Gartner (2012) har 70% av de medverkande organisationerna en policy för BYOD, medan 30% inte har en sådan (se figur 2.2). Nedan kommer vi beskriva vilka för- och nackdelar som präglar införandet av en BYOD-policy.



Figur 2.2 Organisationer som har någon form av BYOD-policy (Gartner, 2012)

2.2.1 Varför tilltalas företag av BYOD?

Det finns flera faktorer som tilltalar företag att tillämpa och införa BYOD på arbetsplatsen. Nedan följder de viktigaste fördelarna med en sådan policy.

- *Lägre kostnader* – Lägre kostnader är den mest uppenbara fördelen med ett företag som tillämpar en BYOD-policy eftersom ledningen inte måste spendera en betydande summa pengar på teknisk utrustning som anställda redan har. Detta skapar besparingar för både större och mindre företag. Dessutom kommer också skador och liknande minska eftersom anställda tenderar att ta bättre hand om sin egen utrustning än företagsägda. Om de förekommer eventuella kostnader, så är anställda villiga att stå upp till en viss summa av kostnader. (BusinessZone, 2013; Cisco, 2013)

- *Teknisk bekantskap* – De flesta anställda tenderar att vara mest bekanta med sin egen utrustning och föredrar därför att använda den. Det kan uppfattas som irriterande för en anställd att börja anpassa sig till en ny typ av teknik. Om företag tillämpar en BYOD-policy så blir detta inte problematiskt eftersom anställda då arbetar med sin personliga utrustning som är anpassat till sina egna behov (BusinessZone, 2013). Enligt CIO Sweden (2012) resulterar detta med ökad produktivitet för anställda.

- *Ökad flexibilitet* – En stor fördel med BYOD är hur flexibelt anställda kan arbeta med sina arbetsuppgifter. Anställda behöver exempelvis inte resa med både företagsägda och personligt ägda enheter eftersom en enhet kommer uppfylla båda kraven. Arbete som vanligtvis enbart kan utföras på arbetsplatsen kommer kunna göras var som helst eftersom anställda redan har tillgång till det material som behövs. (BusinessZone, 2013)

- *Mer frihet* – Om anställda använder företagsägda enheter så måste de ständigt arbeta efter företagets strikta regler för användandet av företagets egendom. Därför skapas det mer frihet för anställda om BYOD tillämpas. (BusinessZone, 2013)

2.2.2 Vilka risker och hot finns med BYOD?

Trots fördelarna med BYOD så kan policyn också medföra flera risker, både för företag och dess anställda. Nedan följer de viktigaste riskerna och hot som företag måste tackla vid införandet av BYOD.

- *Ökade säkerhetsrisker* – Säkerhetaspekterna är det tyngsta motargumentet mot konceptet (Dimensional Research, 2012). Enligt deras undersökning beskrivs anställdas brist på säkerhetsmedvetenhet som det största hotet mot företagsdata.

  Idag är det vanligt att företag spenderar en stor summa pengar på säkerhetssystem eftersom de inte har råd att förlora information eller drabbas av virus. Däremot har anställdas utrustning inte liknande säkerhetsprogram vilket gör utrustningen mer sårbar. Det är mer sannolikt att anställdas utrustning drabbas av skadlig kod än företagsägda, och om dessa sedan kopplas upp mot företagets nätverk kan detta resultera med exponering av företagets information. (BusinessZone, 2013)

- *Utrustningsskillnader* – En annan nackdel med BYOD är att anställda med största sannolikhet har enheter med olika operativsystem som kör olika program. Detta kan orsaka problem för företag eftersom det är svårt att hitta program av hög kvalité som kan implementeras på alla plattformar. Om företag inte tillämpar en BYOD-policy så måste anställda arbeta med företagsägda enheter och då kan företag köpa utrustning som möter deras behov. (BusinessZone, 2013; VMware, 2013)

- *Sammanblandning av information* – Denna utmaning är ett resultat av vilka regler och riktlinjer som existerar kring hur företag väljer att hantera privat information och tjänsteinformation. Det uppstår en problematik när anställdas integritet ställs emot arbetsgivarens kontroller. Det finns det i BYOD-sammanhang en betydande risk för sammanblandning av information vilket ställer särskilda krav på noggrannhet och tekniska begränsningar av olika slag. (Datainspektionen, 2013)

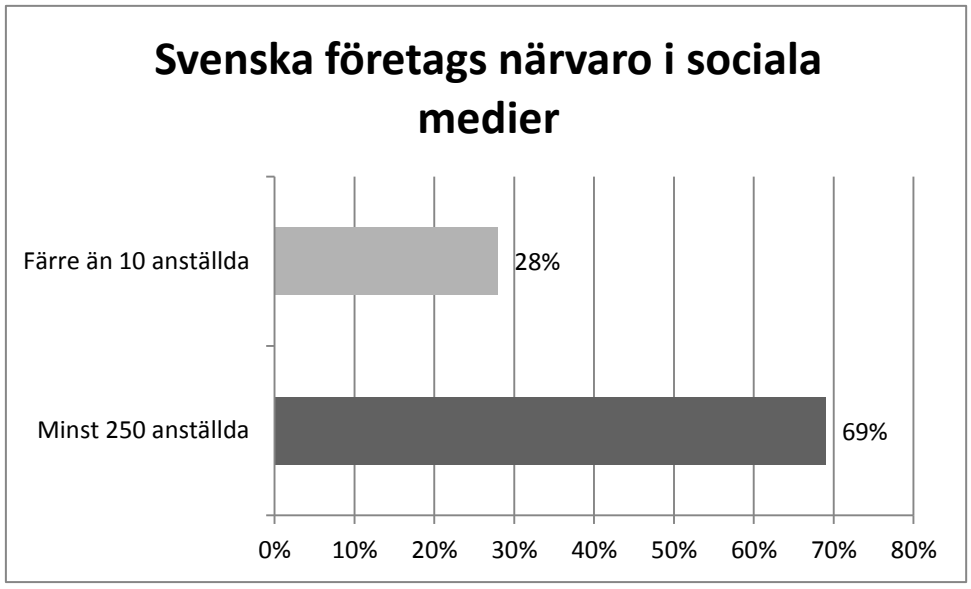
2.3 Sociala medier

Idag är användningen av sociala medier en av de vanligaste formerna av kommunikation människor emellan trots att det är en relativt ny företeelse. Enligt Transportgruppen (2012) så ökar användningen av sociala medier på ett sätt som har kopplingar till arbete och därför är sociala medier relevant för vår studie.

2.3.1 Varför väljer företag att bli aktiva på sociala medier?

Idag väljer alltfler företag att bli aktiva på sociala medier, både nationellt och internationellt. Enligt Statistiska Centralbyrån (2013) närvarar nära hälften av svenska företag på sociala nätverk. Sociala medier definieras som Internetteknologier som kan användas för att skapa och utbyta material internt samt med kunder, leverantörer och andra partners. De vanligaste nätverken är Facebook och Twitter, men även bloggar, mikrobloggar och webbplatser för att dela multimedia blir allt vanligare. (Statistiska Centralbyrån, 2013)

Enligt en undersökning från Statistiska Centralbyrån (2013) närvarar nästan 70% av svenska företag med minst 250 anställda i sociala medier, medan företag med färre än 10 anställda närvarar till 28% (se figur 2.3.1).



Figur 2.3.1 Svenska företags närvaro i sociala medier (Statistiska centralbyrån, 2013)

Det finns flera anledningar till varför företag väljer att bli aktiva på sociala medier. Nedan kommer vi beskriva de viktigaste:

- *Marknadsföring* – Marknadsföring är en av de viktigaste fördelarna med företags närvaro i sociala medier och syftar till att bygga och stärka varumärket. Företag kan publicera sin företagsprofil med syfte att bli mer attraktiva och synas för allmänheten. Detta kan medföra ett bra rykte på marknaden genom att företag visar sin ståndpunkt i relevanta frågor som berör kunder (Stepstone, 2013).

- *Rekrytering av anställda* – Det blir vanligare att använda sociala medier i hela rekryteringsprocessen på flera sätt. Företag kan publicera länkar och platsannonser på nätverken samt locka och söka efter information om potentiella medarbetare och kandidater. Idag är LinkedIn det vanligaste nätverket för rekrytering av nyanställda, följt av Facebook på andra plats (Stepstone, 2013).

- *Service och feedback* – Sociala medier har blivit ett framgångsrikt kommunikationsmedel för att hjälpa kunder. Hemsidor som Twitter och Facebook kan vara en plattform för kunder att interagera med företaget på en mer personlig nivå, istället för att ringa eller kommunicera via e-post. Företag kan via sociala medier visa allmänheten hur hängivna och tacksamma de är för att kunder väljer deras produkter eller tjänster. Dessutom kan kunder dela med sig av sina åsikter vilket kan hjälpa företaget att förbättra sin verksamhet. (LunaMetrics, 2011)

- *Konkurrenter & samarbete* – Sociala medier kan hjälpa företag att hålla reda på sina konkurrenter vilket är viktigt inom alla branscher. Dessutom kan företags närvaro i sociala medier skapa samarbete och partnerskap med ideella organisationer eller andra företag. Detta kan medföra positiva effekter för båda sidorna. (LunaMetrics, 2011)

2.3.2 Lojalitetsplikt och sekretessavtal

Trots att användningen av sociala medier blir allt vanligare och betydelsefull så finns det fortfarande flera faktorer som bekymrar både arbetsgivare och anställda. En problematik som vanligtvis uppstår är arbetstagarens lojalitetsplikt i förhållande till det sekretessavtal som skrivs på tillsammans med arbetsgivaren. (Transportgruppen, 2012)

Transportgruppen (2012) skriver om problematiken:

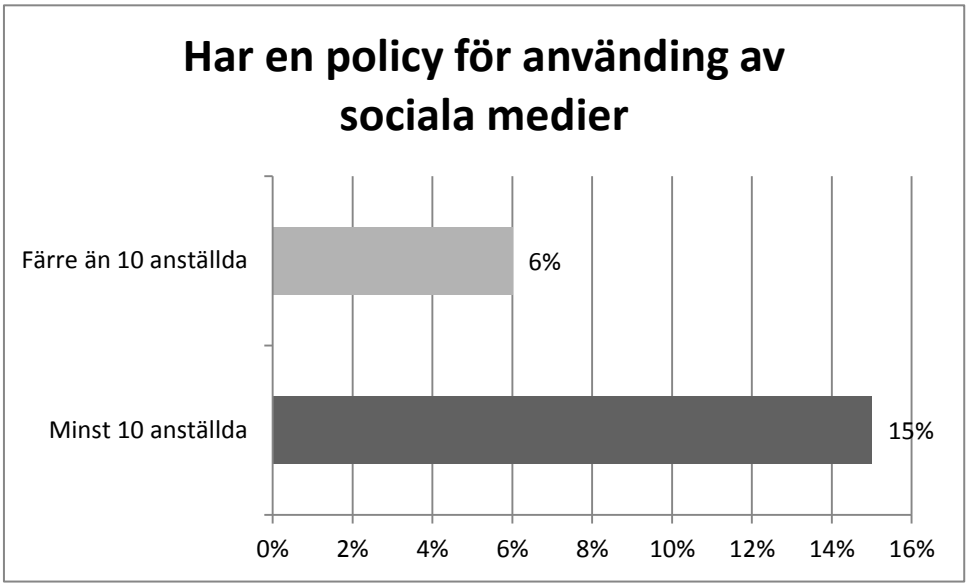
”I varje anställningsavtal ligger en ”tyst reglering” om att arbetstagaren har en lojalitetsplikt i förhållande till arbetsgivaren. Med ”tyst reglering” menas att lojalitetsplikten gäller även om den inte anges uttryckligen i anställningsavtalet.” (Transportgruppen, 2012)

Denna typ av problematik resulterar i att flera arbetsgivare inte vet var gränserna går. För arbetsgivaren är det viktigt att lojalitetsplikten förhindrar anställda att genom olika yttranden skada företaget, eftersom arbetstagaren är anställd dygnet runt. Därför borde lojalitetsplikten

gälla även om den dagliga arbetstiden är slut. Däremot frågar sig flera arbetsgivare hur regler och riktlinjer kan fastställas för anställdas användning av sociala medier på deras fritid. Enligt Findahl (2013) är nästan 66% av Sveriges befolkning på Facebook vilket innebär en risk för sammanblandning av privat information och tjänsteinformation. Frågan om vad anställda får och inte får uttrycka på Facebook, bloggar och andra sociala plattformar har skapat bekymmer för både arbetsgivare och arbetstagare. (Transportgruppen, 2012)

Lojalitetsplikten för anställda i sociala medier skiljer sig från andra plattformar där åsikter och information cirkulerar. En betydande faktor i sociala medier är vilken spridning ett illojalt agerande och uttalande kan få. Den potentiella spridningen och uppmärksamheten är mycket större i sociala medier och därför är företag så pass försiktiga i det hänseendet. (Teknikföretagen, 2013)

I figuren nedan (se figur 2.3.2) visas att det inte är vanligt att svenska företag har en policy för anställdas användning av sociala medier. Det är dock vanligare i företag med fler anställda.



Figur 2.3.2 Har en policy för användning av sociala medier (Statistiska centralbyrån, 2013)

2.3.3 Informations- och yttrandefrihet

Varje medborgare har som grundlagsskyddad rättighet att uttrycka tankar, åsikter och känslor i tal, skrift eller bild (Justitiedepartementet, 1991). Yttrandefrihetsgrundlagen skyddar anställda att uttrycka sina åsikter om exempelvis arbetsgivaren på sociala medier och detta är något som arbetsgivaren måste respektera. Därför är det tillåtet att anställda kritiserar sin arbetsgivare även om detta skulle innebära konsekvenser för företaget. (Transportgruppen, 2012)

I frågan om vad anställda får skriva om företaget i sociala medier råder en problematik mellan kritikrätten och tystnadsplikten. Kritikrätten innebär att anställda kan påtala felaktigheter och missförhållanden hos behöriga myndigheter. Om den anställde vill rapportera ett

arbetsmiljöproblem så är det lagligt att kontakta Arbetsmiljöverket. Däremot innebär tystnadsplikten att den anställde först måste ta upp dessa problem internt med arbetsgivaren innan andra myndigheter blandas in. (Transportgruppen, 2012)

Om den anställde kritiserar sin arbetsgivare eller företaget i syfte att skada eller hämnas så utgör detta ett brott mot anställningsavtalet. Då måste arbetsgivaren haft möjlighet att försvara sig mot den kritik som riktas mot honom/henne. Kritikrätten får alltså inte missbrukas i sådana fall där syftet endast är att skada företaget. (Transportgruppen, 2012)

2.3.4 Hot mot informationssäkerhet

Det finns flera olika hot mot informationssäkerhetsrisker som förknippas med sociala medier. Dessa är de främsta hoten:

- *Skydd av information och privatliv* - Det centrala hotet mot informationssäkerhet i samband med sociala medier är att information som inte ska vara publikt avslöjas eller hamnar i obehörigas händer. Detta kan ske från bland annat användaren antingen genom omedvetenhet eller misstag. Det kan även vara så att användaren själv inte har begått något hot mot sig själv utan i dagsläget är det lätt hänt att andra publicerar eller avslöjar information. (Åbo Akademi, 2012)

- *Spionage* - På sociala medier kan användare obehindrat söka eller hitta information om andra. Därför är det enkelt att spionera på användare av sociala medier. Informationen kan även kopplas ihop med annan information från andra källor. Undersökningar visar att användare är vårdslösa och har alltför stor tillit för sociala medier, detta ökar säkerhetsriskerna vilket är ett utmärkt verktyg för spionage. (Åbo Akademi, 2012)

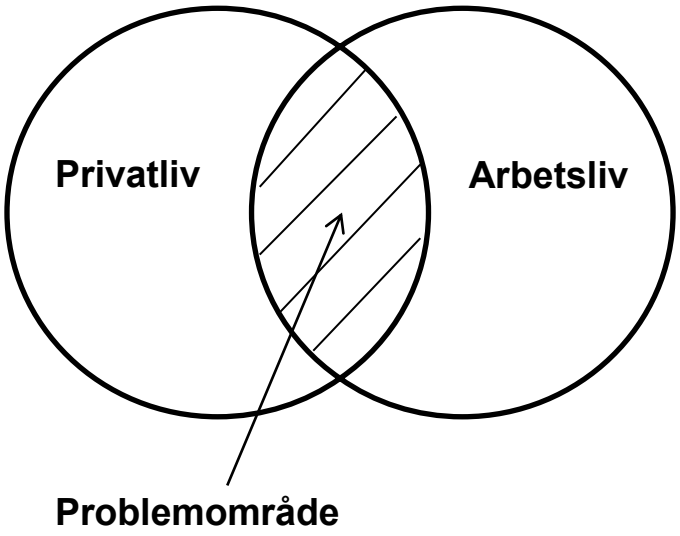
- *Spridning av falsk och felaktig information* på sociala medier kan missbrukas avsiktligt. Det är väldigt vanligt att företag drabbas av falska sidor som härmar företags officiella hemsida, detta gäller även personerna som uppger sig att vara en person som de inte är eller hittat på. (Åbo Akademi, 2012)

- *Stöld av inloggningsuppgifter* - Det är lätt hänt att användare på sociala medier blir av med sina konton genom att bli hackade eller att de hamnar i fel händer. Då är risken stor att dessa personer ställer till med stora skador som exempelvis ändra innehåll, publicera material i deras namn eller företagsnamn, sprida information, stjäla personuppgifter eller företagsuppgifter eller sprida skadeprogram som gör det möjligt för dem att sabotera för andra. (Åbo Akademi, 2012)

- *Virusattacker* - Det sker olika virusattacker mot företag och privatpersoner. Virusattacker sker för att samla information som inte är publikt eller för att skada och fördärva. Virusattacker är så väl organiserade och avancerade att infekterade har svårt att bli av med viruset samt att de infekterade omedvetet kan sprida vidare viruset. (Bilan. C & Hedberg. C, 2001)

2.4 Sammanfattning

Utifrån litteraturgenomgången kan vi definiera vårt problemområde som illusterars i figuren nedan (se figur 2.4). Då anställda enbart använder sociala medier och BYOD i privat bruk samt enbart på arbetsplatsen uppstår inte den problematik som vi behandlar, utan vi är intresserade av den markerade sektionen som är vårt problemområde. Där uppstår gränsdragningsproblematiken med hur regler/riktlinjer bör förhållas i privatlivet gentemot arbetslivet, men även sammanblandning av tjänsteinformation och privat information. Där kommer vårt fokus ligga.

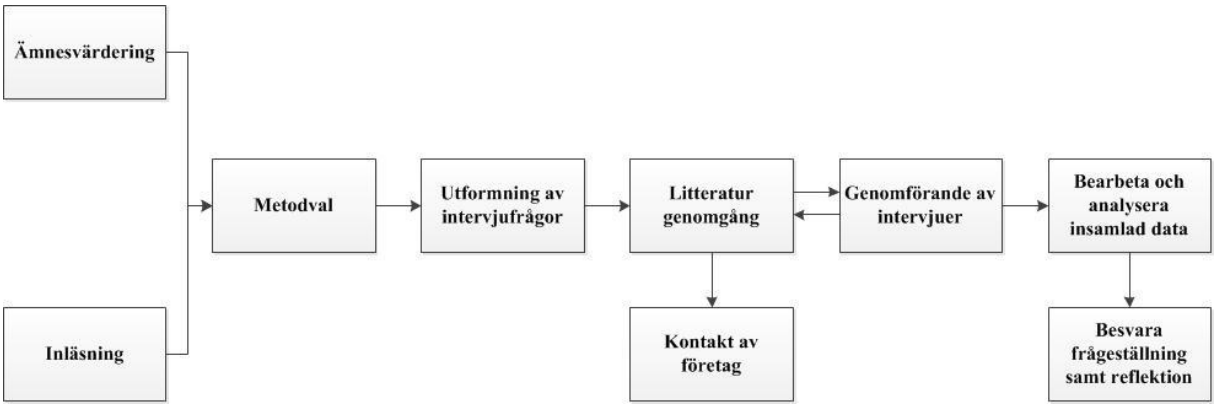


Figur 2.4 Anställdas användning av sociala medier och BYOD

3 Metod

I metoden kommer vi att presentera hur vår bearbetning/process med uppsatsen har gått till. Hur vi har planerat, samlat material och motivation för vår empiriska undersökning. Kapitlet presenterar även hur vi har genomfört våra intervjuer och analyserat dessa samt vilka tekniker som vi har använt.

3.1 Översikt av arbetsprocess



Figur 3.1 Översikt av arbetsprocessen

Steg 1 – Ämnesvärdering

Det första steget i vår arbetsprocess var att besluta om vårt ämnesval var tillräckligt genomtänkt för att genomföra studien. Här genomfördes övergripande diskussioner i gruppen och gemensamt beslutade vi att genomföra en studie om anställdas privata och yrkesverksamma dator-och Internetanvändning.

Steg 2 – Inläsning

Det andra steget syftade till att hitta relevant litteratur, samla material och information om vårt ämnesområde.

Steg 3 – Metodval

Efter ämnesvärderingen och inläsningen påbörjades själva utformningen av uppsatsen genom att välja den metod som lämpar sig bäst för vår studie.

Steg 4 – Utformning av intervjufrågor

Efter metodvalet började vi utforma våra frågor till intervjuerna som var grund till den empiriska undersökningen.

Steg 5 – Litteraturgenomgång/Kontakt av företag
När vi fick intervjufrågorna bekräftade av vår handledare påbörjades vår litteraturstudie

samtidigt som vi kontaktade företag för intervjuer. Arbetet under detta steg skedde parallellt eftersom det oftast tog tid att boka intervjuer.

Steg 6 – Genomförande av intervjuer

Efter att vi arbetade med litteraturgenomgången så genomförde vi de intervjuer som var möjliga. Vi kontaktade någon representant från företaget och utförde intervjuer via telefon, förutom en som genomfördes på plats.

Steg 7 – Bearbeta och analysera insamlad data

Det näst sista steget i arbetsprocessen var att bearbeta och analysera resultatet från våra intervjuer.

Steg 8 – Besvara frågeställning samt reflektion

Det avslutande steget i arbetsprocessen var att föra en diskussion och reflektera kring resultatet av vår empiriska undersökning kopplat till vårt teoretiska ramverk. Frågeställningen som vi utformade i början av projektet besvarades sedan i detta steg.

3.2 Kvalitativ metod

Vi valde en kvalitativ undersökningsmetod för att besvara vår forskningsfråga. Vår studie syftar inte till att uppnå ett resultat av en definitiv sanning, utan snarare att utforska hur företag påverkas av anställdas privata och yrkesverksamma dator- och Internetanvändning och den komplexa miljön som företagen måste förhålla sig till. Därför blev det ett naturligt val att använda en kvalitativ undersökningsmetod eftersom den lämpar sig bättre då forskarna vill skapa djupare förståelse i ett oklart ämne (Jacobsen 2002).

3.3 Val av respondenter

Vår undersökning innefattar fyra intervjuer med svenska företag som är närvarande på sociala medier. Företagen valdes ut efter att vi kontrollerade deras bakgrund och fastställde att de var involverade i sociala medier. Vi har intervjuat företagens VD eller IT-ansvariga eftersom dessa endast kunde besvara våra frågor. En översiktlig bild av företagen ges i tabell 3.3.

	Respondent 1	Respondent 2	Respondent 3	Respondent 4
Huvudkontor	Lund	Stockholm	Lund	Lund
Organisationstyp	Medelstort	Stort	Litet	Litet
Inriktning	Teknikkonsult-företag	IT-Tjänster	Webbbaserade tjänster	Ekonomiska frågor
Intervjuperson	R1	R2	R3	R4

Tabell 3.3 Sammanfattande tabell över de intervjuade respondenterna

3.4 Intervjuteknik

Inledningsvis hade vi tänkt genomföra samtliga intervjuer med respondenterna på plats, men insåg sedan att detta inte var möjligt. De respondenter som accepterade att genomföra en intervju om vår studie föredrog att göra detta via telefon. Däremot fanns det en respondent som faktiskt föredrog om vi kunde besöka honom på plats. Detta uppfattade vi som positivt eftersom vi fick möjlighet att utforska båda intervjuteknikerna.

Det finns flera anledningar till varför vi inledningsvis ville genomföra intervjuerna på plats. Vi anser att vi kunde få en bättre koppling och relation till respondenten genom att tala öga mot öga, vilket förhoppningsvis skulle resultera i ett ärligare och utförligare svar. Vår förhoppning var att respondenterna hade uppfattat undersökningen som mer seriös om vi hade varit på samma plats, vilket skulle motivera de att hjälpa oss med uppsatsen.

Enligt Jacobsen (2002) kan intervjuer som utförs öga mot öga resultera i att vi som undersöker påverkas av miljön och därmed tappar att betrakta fenomenet objektivt. Detta anser vi inte var relevant i vårt fall eftersom syftet med vår studie inte var att uppnå ett resultat i form av en definitiv sanning, utan snarare att utforska den problematik som kan uppstå med anställdas dator- och Internetanvändning. Därför använde vi oss av semistrukturerade intervjuer för att ge respondenterna chans att säga sin åsikt i frågan. Semistrukturerade intervjuer tillåter respondenten att utveckla sina svar och gör intervjun mer flexibel, vilket var något som vi eftersträvade. Vi kunde tydligt anmärka att respondenterna som intervjuades på plats var mer villiga att ge detaljerade och utförligare svar. Det syntes tydligt att de ville ge oss en bredare bas att utgå ifrån till analysen, vilket vi naturligtvis uppskattade.

Jacobsen (2002) menar även att besöksintervjuer kan påverka svaren från respondenterna eftersom de kan bli påverkade av den fysiska närvaron. Dessutom visste vi att vårt ämnesval kunde uppfattas som känsligt och förundrades över hur ärliga respondenterna skulle vara. Däremot uppfattade vi stämningen som avslappnad och lyckades utföra en bra intervju med utförliga svar och diskussioner. Vi började intervjuerna, både telefon- och besöksintervjuerna, med att berätta att företagen och respondenterna kunde förbli anonyma i vår studie och detta var något som samtliga ville.

3.5 Intervjuguide

Fråga 1 – Finns det regler/riktlinjer eller en form av Internetpolicy för anställdas dator- och Internetanvändning?
– Exempelvis vad han/hon skriver på sociala medier?
– Hur tänkte ni då ni bestämde reglerna/riktlinjerna?
– Eller, hur tänkte ni då ni inte satt upp några regler?

Denna inledande frågan täcker en central del av vår studie. Vår förhoppning var att respondenterna tydligt svarade om det fanns regler för anställdas dator- och Internetanvändning samt förklarar varför reglerna fanns eller inte behövdes.

Fråga 2 – Finns dessa regler/riktlinjer dokumenterade?
– Får anställda information om reglerna/riktlinjerna?
– Hur får anställda information om reglerna/riktlinjerna?

Denna fråga kunde endast besvaras om respondenterna svarade ja på föregående fråga. Om det fanns regler för anställdas dator-och Internetanvändning, blev det viktigt för oss att veta om policyn var dokumenterad eller inte. Om respondenterna svarade ja, så måste även företagets anställda ta del av reglerna. Vi var intresserade av att veta om reglerna skickades till alla anställda samt hur de fick tillgång till informationen.

Fråga 3 – Sker det någon kontroll av anställdas dator- och Internetanvändning?
– Om ja, finns det regler/riktlinjer för hur en sådan kontroll ska ske?
– Om nej, finns det någon anledning varför ni avstår att övervaka?
– I vilket syfte görs dessa kontroller?

Även denna fråga täcker en central del av vår studie och kunde besvaras oavsett om svaret på första frågan vore ja eller nej. Om det fanns regler/riktlinjer för hur en kontroll skulle ske, så förväntade vi oss ett utförligt svar från. Vi försökte också ta reda på varför sådana kontroller anses vara nödvändiga.

Fråga 4 – Oroar ni er för att era anställda ska göra bort sig på nätet/publicera olämpliga saker på arbetstid?
– Om ja, gör ni något åt detta?
– Om inte, kommentera gärna det också!

Syftet med denna fråga var att få en överblick över om företag på något sätt bekymrar sig om anställdas aktiviteter på Internet, främst på arbetsplatsen. Frågan var viktig eftersom svaret från respondenterna kunde bli en central analysfaktor.

Hur känner ni om anställdas surfvanor och Internetanvändning på sin fritid?
***–** Är det något som bekymrar er?*
***–** Har ni regler/riktlinjer för hur anställda ska uppföra sig på sin fritid?*
***–** Händer det att era medarbetare på fritiden direkt eller indirekt representerar sin arbetsgivare eller företaget?*

Syftet med denna fråga liknar föregående fråga men fokus ligger istället på anställdas dator- och Internetanvändning på fritid. Vår förhoppning var att respondenterna tydligt förklarar den syn som företaget har på anställdas surfvanor och om detta är bekymrande på något sätt. Vi försökte också ta reda på om anställda på något sätt måste representera sin verksamhet på sin fritid eller om företaget inte ställer sådana krav.

Fråga 6 – Vad tycker ni om anställdas egna tekniska utrustning (BYOD)?
– Finns det några problem som ni ser?
– Finns det några fördelar?

Denna fråga var viktig eftersom en aspekt av vår studie behandlar BYOD och vår förhoppning var att respondenterna berättade sin syn på ämnet. Vi frågade om företaget kunde identifiera både för- och nackdelar med anställdas egna tekniska utrustning på arbetsplatsen.

Fråga 7 – Finns det exempel på tidigare händelser där anställdas dator- och Internetanvändning har skapat problem för företaget?
– Förklara gärna!
– Hur påverkas företaget av händelsen?
– Skedde det några förändringar efteråt?

Om respondenterna kunde svara på frågan så förväntade vi oss ett utförligt svar eftersom ett sådant exempel kunde bli en viktig analysfaktor i uppsatsen. Vi frågade också hur en sådan händelse påverkade verksamheten och om företaget genomförde förändringar för att det inte skulle upprepas.

3.6 Analys av insamlad data

För att få en strukturerad och detaljerad intervju som möjligt var vi tvungna att göra dem kvalitativa. Syftet med intervjuerna var att få en förståelse för hur företagen påverkades av anställdas privata och yrkesverksamma dator- och Internetanvändning. Innan varje intervju hade vi redan framhävt en viss kontakt med respektive representant från företagen och förklarat vår uppsats och hur vår empiriska undersökning var upplagd. Detta för att få en kontakt och närhet med intervjupersonerna samt för att få tillit för varandra och kännas sig trygga. Varje intervju började vi med att berätta för dem om de föredrog att vara anonyma eller inte för att få utförligare svar.

För att kunna analysera intervjuerna så noggrant och detaljerat som möjligt började vi med att berätta för dem att vi ville spela in intervjuerna för vår egna och rapportens precisions skull. Samtidigt som intervjuerna pågick gjordes kontinuerliga anteckningar för att få en egen uppfattning samt bild över hur intervjupersonerna tänkte och kände i varje ögonblick av

intervjuprocessen. Varje intervjuteknik som genomfördes var på grund av att vi ville vara så strukturerade som möjligt för att det skulle bli lättare för oss att analysera och kategorisera intervjuerna senare i empirin.

Efter varje intervju gick vi noggrant igenom inspelningen och anteckningarna var för sig för att sedan gör en detaljerad transkribering av intervjun. Transkriberingarna gick vi sedan igenom för att dubbelkolla så att vi inte har missat något. Vi ansåg att det var väldigt viktigt att gå igenom intervjuinspelningarna och transkriberingarna flertal gånger för att inte ha missat något. Det är väsentligt att denna process bearbetades korrekt för rapportens framtida analyser och diskussioner.

Därefter gick vi igenom varje transkribering och anteckningar gjordes individuellt utifrån det material man ansåg var viktigast med respektive intervju. Såhär fördubblade vi materialet och kunde få dubbla synvinklar på varje intressant aspekt i materialet. Utifrån intervjusvaren analyserade vi likheter och skillnader.

3.7 Kritik av metodval

Våra intervjumetoder var besöksintervju och telefonsintervju och det finns både negativa och positiva aspekter om bådadera. Att genomföra individuella besöksintervjuer är tidskrävande enligt Jacobsen (2002), vilket vi kan se i våra bilagor att de tre första bilagorna som var telefonintervjuer var inte lika långa som den ena besöksintervjun. Det kan ta väldigt lång tid att planera upp en besöksintervju för man ska planera och lägga ner en massa tid, exempelvis som att fixa rum där intervjun kan ske. Det tar ofta lika lång tid att ordna en besöksintervju som att genomföra den (Jacobsen, 2002). Besöksintervjuer ger även stora datamängder i form av anteckningar och inspelningar. Det finns även risker för att det kommer bli så mycket information att man inte kan hantera eller få överblick över den (Jacobsen, 2002). Vidare vad som gäller för telefonsintervjuer kan det vara att intervjupersonerna tycker det är lättare att tala om känsliga ämnen i intervjuer öga mot öga än i telefon (Jacobsen, 2002). Anledningen är att det blir lättare för personer att få personlig kontakt när de fysiskt sitter mitt emot varandra, det skapas en förtrolig stämning. Det blir även lättare för intervjupersonen att ljuga eller undvika sanningen i en telefonintervju. Över telefonintervjuer förlorar intervjuaren möjligheten att observera hur intervjupersonen uppträder vid en telefonsintervju (Jacobsen, 2002).

4 Empiri och analys

I detta avsnitt presenteras resultatet av vår kvalitativa undersökning samt analys av detta material. Vi kommer presentera resultatet av intervjuerna, följt av en första analys som kommer ligga till grund för den fördjupande diskussionen i nästa kapitel. Vi har intervjuat fyra svenska företag som arbetar inom olika branscher och samtliga av företagen har valt att förbli anonyma i undersökningen. Vi kommer därför benämna företagen som R1 (Respondent 1), R2 (Respondent 2), R3 (Respondent 3) och R4 (Respondent 4) framöver.

En viktig anmärkning som berör R4 är att intervjun bestod av två delar. Det var tänkt att vi enbart skulle intervjua företagets VD men blev senare informerade att personen var på möte, och då fick vi istället intervjua företagets dataansvarig. Vi intervjuade den personen och fick svar på våra frågor, men i slutet av intervjun blev VD:n tillgänglig och vi fick ett par minuter med honom. Intervjun med VD:n utvecklades mer till en diskussion där han presenterade sina åsikter kring frågorna som vi utformat, istället för att svara lika konkret som den dataansvarige gjorde. Framöver kommer svaren från VD:n att specificeras i texten, medan de grundläggande svaren baseras på intervjun med den dataansvariga.

4.1 Fråga 1 av 7 – Internetpolicy & Sociala medier

Finns det regler/riktlinjer eller en form av Internetpolicy för anställdas dator- och Internetanvändning?
– Exempelvis vad han/hon skriver på sociala medier?
– Hur tänkte ni då ni bestämde reglerna/riktlinjerna?
– Eller, hur tänkte ni då ni inte satt upp några regler?

4.1.1 Resultat

På första frågan om företagen hade regler/riktlinjer för anställdas dator- och Internetanvändning skiljer sig svaren en del. R1 har ett regelverk för hur anställda får använda företagets resurser och hur de fick agera ute på nätet. Däremot hade företaget inte specificerat vad anställda får och inte får skriva. Företaget medger att det är en självklarhet att anställda inte får befinna sig på platser eller vara involverade i aktiviteter som är olagliga eller oetiska.

I följdfrågan om hur företaget bestämde reglerna svarade R1 att de inte har något intresse av att bryta mot lagen och inte vill att bolagsnamnet ska förknippas med något som företaget inte står för. Företagets utrustning och namn får inte användas i sammanhang som strider mot företaget grundvärderingar och normer. Däremot medger R1 att om någon enskild person vill uttala sig politisk eller rasistisk så ska detta göras som privatperson och inte på något sätt förknippas med företaget.

För att få en klarare bild över hur R2 resonerar kring anställdas dator- och Internetanvändning valde vi att beakta svar från flera frågor i intervjun. Detta gjorde vi för att vi misstänker att R2 missuppfattade oss i början av intervjun. R2 medger att de har en allmän Internetpolicy i företaget, men inga regler/riktlinjer för hur anställda ska förhålla sig till sociala medier. Däremot håller företaget på att utforma en policy för anställdas användning av sociala medier

eftersom ämnet blir alltmer aktuellt, men företaget anser samtidigt att användning av sociala medier utanför företaget bör baseras på sunt förnuft. I följdfrågan svarade R2 att det är en självklarhet för ett bolag av deras storlek och position att ha en Internetpolicy.

R3 medger att de inte har regler/riktlinjer för anställdas dator- och Internetanvändning. I följdfrågan om varför de inte satt upp några regler medger företaget att bolaget är för litet för att en sådan Internetpolicy ska behövas, och att samtliga i företaget arbetade med sunt förnuft. Även R4 saknade några skriftliga regler för anställdas dator- och Internetanvändning och förklarade att det inte behövdes och att ingen i företaget har tänkt på det.

4.1.2 Analys

En grundläggande analys som kan göras är att de två större företagen, R1 och R2, har en form av Internetpolicy för anställdas dator- och Interneranvändning, medan de mindre företagen, R3 och R4, anser att de inte behöver en Internetpolicy ännu. Företagets storlek är alltså en betydande faktor om regler/riktlinjer för dator- och Internetanvändning anses vara nödvändigt eller inte.

I frågan om sociala medier var företagen inte lika tydliga. Trots R2s storlek så har företaget inte några regler/riktlinjer för hur anställda ska förhålla sig till sociala medier, men håller däremot på att utforma en sådan policy. Det finns nämligen ett behov av en sådan policy enligt R2:

”Nej, det är ju det att sociala medier exploderar. Sen börjar man prata om incidenter och allt till arbetslivet som inte får och ska komma ut. Det är därför vi tittar mer på det just nu.” (Bilaga B2, s. 46).

R1, R3 och R4 hade inte heller några regler/riktlinjer för användningen av sociala medier, både i arbets- och privatlivet. Däremot betonade R1 att om anställda vill begå brott eller uttala sig politiskt, rasistiskt eller på något sätt som inte stämmer överens med företagets värdegrund, så görs detta som privatperson. R3 och R4 litade på sina anställda men svarade att olämpligheter i sociala medier utförs som privatperson likaså. R1, R3 och R4 ser alltså inget behov av att reglera hur anställda ska förhålla sig till sociala medier, medan R2 istället börjar uppmärksamma att det behövs en policy för användningen av dessa plattformar.

4.2 Fråga 2 av 7 – Dokumentation av Internetpolicy

Finns dessa regler/riktlinjer dokumenterade?
– Får anställda information om reglerna/riktlinjerna?
– Hur får anställda information om reglerna/riktlinjerna?

4.2.1 Resultat

R1 svarar att reglerna/riktlinjerna finns dokumenterade i företagets ledningssystem som är certifierade. Där finns företagets styrdokument som beskriver hur företaget jobbar. Nyanställda måste skriva på en blankett där alla förhållningsregler och liknande finns nertecknade och om dessa godkänns så försäkrar företaget att den nyanställde lever upp till

alla policydokument och inte överträder dessa. Företaget har också i samband med anställningen ett introduktionsmöte där nyanställda får information om alla möjliga typer av regler.

R2 medger att alla olika dokument som reglerar hur företaget och anställda ska arbeta finns på företagets hemsida och att samtliga anställda måste läsa igenom informationen. Dessutom måste nyanställda skriva på att de tänker följa alla regler/riktlinjer i början av anställningsprocessen.

Eftersom R3 och R4 inte har en Internetpolicy för anställdas dator- och Internetanvändning så finns inte denna heller dokumenterad. Därför kunde R3 och R4 inte svara på frågan.

4.2.2 Analys

Gemensamt för R1 och R2 är att Internetpolicyn finns dokumenterad och att anställda får ta del av informationen. Båda företagen behövde en underskrift från den nyanställde för att försäkra sig om att de accepterar företagets villkor och inte tänker överträda dessa. Därmed får anställda information om Internetpolicyn samt blir informerad om denna i början av anställningsprocessen. R2 svarade även att samtliga dokument som reglerar hur företaget och dess anställda ska arbeta finns öppet för allmänheten på deras hemsida, medan detta var något som R1 inte pratade om.

Denna fråga är inte relevant för R3 och R4 och därför kunde inga slutsatser dras.

4.3 Fråga 3 av 7 – Övervakning & Kontroll

Sker det någon kontroll av anställdas dator- och Internetanvändning?
– Om ja, finns det regler/riktlinjer för hur en sådan kontroll ska ske?
– Om nej, finns det någon anledning varför ni avstår att övervaka?
– I vilket syfte görs dessa kontroller?

4.3.1 Resultat

R1 kontrollerar inte vad anställda skriver, men kontrollerar vilka hemsidor som besöks och vad som laddas ner. Däremot sker det inte någon form av kontinuerlig sticksprovskontroll eller övervakning över anställdas vardagliga rutiner. Syftet med övervakningen grundar sig på att anställda har tillgång till företagets utrustning och därför sker övervakningen enbart på arbetsplatsen. R1 anser att anställda bör förstå att reglerna för företagets tekniska utrustning även sker utanför kontoret. Däremot medger R1 att företaget inte har några skriftliga dokument på hur en sådan övervakning ska ske, men det framgår i Internetpolicyn att det utförs kontroller på företagets tekniska utrustning.

R2 kontrollerar inte alls vad anställda skriver på nätet och anser att det är sekretesskränkande att företag går in och övervakar vad anställda skriver på sociala medier och liknande. Däremot kontrollerar företaget datorerna, exempelvis om de blir stulna. Annars sker ingen kontroll eller övervakning.

R3 och R4 svarade att de inte på något sätt övervakar eller kontrollerar anställdas dator- och Internetanvändning. R3 anser att sådan övervakning inte skulle hjälpa företaget och R4 anser att det inte finns någon anledning att övervaka företagets anställda på grund av antalet anställda. R4 medger att sådan kontroll inte behövs eftersom företaget kan mäta anställdas resultat. Om resultatet inte presenterades i tid så är det uppenbart att den anställde inte har jobbat med sina arbetsuppgifter. R3 svarade att de litar på samtliga anställda och därför behövs ingen övervakning eller kontroll.

4.3.2 Analys

R2, R3 och R4 kontrollerar inte anställdas dator- och Internetanvändning och anser att sådan övervakning inte behövs. R2 anser dessutom att sådan övervakning är sekretesskränkande för anställda vilket kan tolkas som överraskande med tanke på deras storlek och aktivitet på sociala medier. R3 och R4 grundar sitt ställningstagande i frågan på företagets storlek och förstår inte hur företaget skulle gynnas av en sådan kontroll. Detta innebär att företagens storlek är en betydande faktor i frågan, trots att R2 inte kontrollerar någonting utöver datorerna.

R1 är det enda företaget som har en typ av kontroll, men medger samtidigt att det inte finns några regler/riktlinjer för hur en sådan kontroll ska ske, trots att företaget har en Internetpolicy. Det framgår i Internetpolicyn att R1 kontrollerar företaget utrustning, men inte att de kontrollerar vilka filer som laddas ner samt vilka hemsidor som besöks. Företaget medger att de inte kontrollerar anställdas vardagliga rutiner men hävdar samtidigt att om företagets utrustning används så gäller reglerna även utanför arbetstid:

”Däremot har vi ju alltid möjlighet att se om någonting inte har hanterats på vårt sätt. Då kan vi se saker som skett utanför arbetstid eller arbetsnätverket, men som sagt ingen kontroll sker bara sådär.” (Bilaga B1, s. 42).

4.4 Fråga 4 av 7 – Anställdas dator- och Internetanvändning på arbetstid

Oroar ni er för att era anställda ska göra bort sig på nätet/publicera olämpliga saker på arbetstid?
– Om ja, gör ni något åt detta?
– Om nej, kommentera gärna det också!

4.4.1 Resultat

I frågan om företagen oroar sig för anställdas aktivitet på nätet svarade R1 att de inte oroar sig eftersom deras anställda är högt utbildade och kompetenta i sitt arbete. De vet vad som får skrivas och vad som inte får skrivas. Däremot medger R1 att det alltid kan finnas någon som missförstått reglerna och som bryter mot dessa medvetet eller omedvetet, men detta är något som företaget inte tänker på särskilt mycket.

R2 oroade sig inte över anställdas aktivitet på nätet och betonade att allt som anställda väljer att skriva på sociala medier och liknande är privat. Däremot medger R2 att om anställda

skriver olämpliga saker om företagets eller om företagets kunder som sedan sprider sig på ett informellt sätt, så måste arbetsgivaren agera. Detta finns det däremot inget regelverk för. Företaget har en uppförandekod (code of cunduct) som beskriver hur anställda ska agera och uppföra sig mot kunder och leverantörer. Det regelverket är något som samtliga anställda har skrivit på och måste följa.

R3 och R4 svarade att de inte oroar sig för anställdas aktivitet på nätet. R4 skriver till och med att de inte tänker på den frågan. Båda företagen hade inte mycket att kommentera i den frågan.

4.4.2 Analys

Samtliga företag oroar sig inte över anställdas aktivitet på nätet eller att anställda ska publicera olämpliga saker. R1 och R2 medger däremot att det alltid finns en chans att något liknande kan ske, men det är inget som är oroande. En intressant anmärkning är att R2 är det enda företaget som har ett regelverk för hur anställda ska agera och uppföra sig socialt mot kunder och leverantörer, medan resterande företag inte har något liknande. R1 har med största sannolikhet inte någon uppförandekod eftersom företaget anser att deras anställda är tillräckligt kompetenta och utbildade för att något oroande ska inträffa. Detta kan uppfattas som märkvärdigt.

4.5 Fråga 5 av 7 – Anställdas dator- och Internetanvändning på fritid

Hur känner ni om anställdas surfvanor och Internetanvändning på sin fritid?
– Är det något som bekymrar er?
– Har ni regler/riktlinjer för hur anställda ska uppföra sig på sin fritid?
– Händer det att era medarbetare på fritiden direkt eller indirekt representerar sin arbetsgivare eller företaget?

4.5.1 Resultat

R1 har inte utformat några speciella regler för hur anställda ska uppträda på sin fritid. Om anställda exempelvis väljer att bära en bolagströja eller köra en av företaget bilar så förutsätter ledningen att den anställde inte bryter mot företagets grundläggande värderingar och dessa värderingar gäller även för anställdas privata användning av Internet. R1 vill inte att anställda på något sätt ska uppföra sig på ett sätt som kan skada företagets namn, men några regler/riktlinjer för anställdas privata dator- och Internetanvändning finns inte.

R2 har inte heller utformat några regler/riktlinjer för anställdas privata dator- och Internetanvändning, men däremot är det något som kan vara bekymrande eftersom de finns representerade på flera olika sociala medier där anställda också befinner sig. Företaget har inte något regelverk i frågan om vilka hemsidor och liknande anställda får och inte får besöka på sin fritid, men betonar att anställda inte får uppträda på ett sätt som kan var skadligt för företaget på Internet. Precis som användningen av Internet på arbetstid så kommer arbetsgivaren att agera om olämpliga saker skrivs om företaget, trots att det är privat. Däremot är detta ingenting som övervakas.

Precis som i frågan om anställdas dator- och Internetanvändning på arbetstid, svarade R3 och R4 att de inte tänker på vad anställda publicerar på sin fritid. De förutsätter att företagets anställda föregår med gott exempel.

4.5.2 Analys

Gemensamt för företagen är att de inte utformat en policy för anställdas privata dator- och Internetanvändning. R3 och R4 tänker inte ens på vad anställda skriver eller publicerar på sin fritid och detta beror med största sannolikhet på företagens storlek. Företagen har inte tillräckligt många anställda för att arbetsgivaren ska behöva utforma regler/riktlinjer för hur de ska uppföra sig på sin fritid.

De största företaget i undersökningen, R2, har inte heller utformat några regler/riktlinjer men medger dock att anställdas privata användning av sociala medier kan vara bekymrande. Detta är inte allt för överraskande eftersom R2 nyligen bestämt sig för att utforma en policy för anställdas användning av sociala medier. R2 anser alltså att det finns ett behov att reglera hur anställda förhåller sig till sociala medier vilket resterande företaget inte ser ännu.

R1 vill inte att anställda ska representera företaget på ett olämpligt sätt men har inte utformat en policy för privat användning av Internet. R1 anser med största sannolikhet att det inte behövs eftersom de litar på sina anställda och anser att de är tillräckligt kompetenta för att inte göra bort sig.

4.6 Fråga 6 av 7 – BYOD

Vad tycker ni om anställdas egna tekniska utrustning (BYOD)?
– Finns det några problem som ni ser?
– Ser ni några fördelar?

4.6.1 Resultat

I frågan om BYOD svarade R1 att anställda får tag med sig personlig utrustning till arbetsplatsen, men får inte koppla utrustningen till företagets nätverk eller server. Anledningen till varför utrustningen inte får kopplas till nätverket är företagets kraftiga sekretesspolicy gentemot obehöriga. Företaget har specifika sekretessavtal med kunder som innebär att information inte får spridas till obehöriga, och dessa avtal tar R1 på stort allvar. Lokaler på arbetsplatsen och liknande får dessutom inte heller besökas av obehöriga. De regler/riktlinjer som företaget har gällande BYOD finns reglerade i företagets Internetpolicy.

R2 påstår att anställda får tag med sig personlig utrustning till arbetsplatsen och att BYOD är ett aktuellt ämne som innebär en del utmaningar för företaget. R2 stoppar inte anställda från att tag med sig sin utrustning, men föredrar att de använder företagets enheter. Företagets enheter får endast kopplas till nätverket eftersom de är installerade med särskilda säkerhetsprogram. Om utrustning blir stulen kan företaget utföra en blockeringsfunktion som gör utrustningen funktionsoduglig. Därför kan obehöriga inte få tillgång till företagets information om deras egna enheter används. R2 har en BYOD-policy där samtliga

regler/riktlinjer för anställdas personliga utrustning finns reglerade. Företaget har dessutom en MDM-lösning (mobile device management) som säkerställer säkerheten kring företagsinformation mobilt.

R3 tillåter anställda att tag med personlig utrustning till arbetsplatsen och koppla dessa mot företagets nätverk. Företaget ser endast fördelar med BYOD eftersom det aldrig tidigare skett några problem i den frågan. R3 menar att det enbart är en fördel om anställda har de datorer som de är vana vid att använda och den utrustning som de själva vill ha.

Även R4 tillåter anställda att tag med sig personlig utrustning till arbetsplatsen och koppla dessa mot företagets nätverk. Däremot har det aldrig hänt att anställda tagit med sig egna datorer, utan tangentbord, skärmar och liknande är vanligare för bekvämhetens skull. Det har aldrig skett någon form av incident tidigare i frågan om BYOD.

4.6.2 Analys

Gemensamt för samtliga respondenter är att alla tillåter anställda att tag med sig sin personliga utrustning till arbetsplatsen, men i frågan om de får koppla sig mot företagets nätverk, skiljer sig svaren en del. R1 och R2 tillåter inte anställda att koppla sin personliga utrustning mot företagets nätverk, medan R3 och R4 inte ser några problem i frågan. R1 är bekymrade i frågan eftersom företaget har speciella sekretessavtal med kunder som gör att de inte vill ta några risker. R2:s svar angående säkerheten är ett tecken på att företaget inte anser att anställdas personliga utrustning är säkert nog för att kopplas mot företagets nätverk. Både R1 och R2 är oroliga över att information hamnar i fel händer och därför tillåter inte företagen att anställda får koppla sina enheter mot respektive nätverk. Dessutom har båda respondenterna ett regelverk som beskriver hur användningen av BYOD ska tillämpas.

I frågan om anställda fick koppla sin utrustning mot företagets närverk medger R3 och R4 att de inte ser några problem. Företagen har inte utformat någon BYOD-policy utan anställdas rätt att använda personliga enheter är relativt fritt. Båda företagen är optimistiska i frågan och ser fördelar mer än nackdelar. Däremot svarade R4 att anställda inte tagit med sig datorer till arbetsplatsen ännu vilket kan uppfattas som märkligt.

4.7 Fråga 7 av 7 – Tidigare incidenter

Finns det exempel på tidigare händelser där anställdas dator- och Internetanvändning har skapat problem för företaget?
– Förklara gärna!
– Hur påverkades företaget av händelsen?
– Skedde det några förändringar efteråt?

4.7.1 Resultat

R1 delade en incident som inträffade i slutet av 1990-talet där företaget tvingades samarbeta med polisen för att utreda ett fall. Företaget hade ett samröre i ett gemensamt projekt som behandlade olika typer av utbildningar, såsom arbetsmarknadsutbildningar, högskoleutbildningar och företagsutbildningar. Då hade företaget ett elevnätverk och ett

personalnätverk på respektive ort som var separata från varandra. R4 blev kontaktade av polisen eftersom någon hade via personalnätverket behandlat pornografiska hemsidor. Det visade sig vara en anställd som besökt pornografiska hemsidor under dessa utbildningstillfällen. När företaget blev uppringt av polisen hade de ingen aning om vad som hade hänt.

I följfrågan om hur R1 påverkades av händelsen och vilka åtgärder som gjordes efteråt, svarar företaget att utåt förändrades inte särskilt mycket eftersom det endast var ett fåtal personer som kände till incidenten. Internt behövde företaget blockera vissa hemsidor i både personal- och elevnätverket vilket gjorde att företaget påverkades av händelsen eftersom något liknande aldrig tidigare inträffat.

R2 svarar att det säkerligen inträffat flera incidenter eftersom företaget har tusentals anställda och är verksamma i flera länder. Ett exempel som R2 delade var att flertal datorer blivit stulna de senaste åren vilket företaget anser är allvarligt eftersom anställda då inte följer de regler/riktlinjer som utformats i policyn. Lyckligtvis är företagets datorer installerade med särskilda säkerhetsprogram som gör det möjligt att blockera obehöriga att få tillgång till information. Nyligen blev däremot en dator stulen där säkerhetsprogramvaran inte var installerad och detta orsakade stora konsekvenser för företaget. Däremot ville R2 inte diskutera vilka åtgärder som utfördes efter incidenterna.

R3 och R4 har aldrig tidigare upplevt en incident där anställdas dator- och Internetanvändning på något sätt skapat problem för företaget. R4 medger igen att företaget kan mäta anställdas resultat och någon tidigare incident frågan har ännu inte inträffat.

4.7.2 Analys

R1 och R2 har upplevt tidigare incidenter där anställdas dator- och Internetanvändning skapat problem för företagen och detta resulterade i att respektive företaget fick agera. Den incident som påverkade R1 kan vara en av anledningarna till varför företaget har en sådan strikt BYOD-policy där anställda inte får koppla sin personliga utrustning mot företagets nätverk. R2 betonar tydliga säkerhetsbrister i den utrustning som anställda väljer att tag med sig och därför får de inte kopplas mot företagets nätverk. Båda respondenterna värnar om sin information och vill inte att obehöriga ska få tillgång till något sekretessbelagt material.

4.8 Observation av företagsstorlek

Utifrån vårt undersökningsmaterial kan vi tydligt konstatera att det finns en uppenbar skiljelinje i svaren mellan större och mindre företag. Denna observation kommer återkomma och analyseras i uppsatsen diskussionskapitel och slutsats.

5 Diskussion

I detta kapitel kommer de resultat som erhölls genom föregående kapitel att diskuteras närmare med stöd av uppsatsens teoretiska ramverk. Detta kapitel kommer liksom i föregående kapitel att följa strukturen efter de sju ämnesområden som utformats.

5.1 Internetpolicy & Sociala medier

I frågan om Internetpolicy undersökte vi om respondenterna hade skriftliga dokument som reglerar anställdas privata och yrkesverksamma dator- och Internetanvändning samt varför en sådan policy behövdes. Utifrån resultatet som erhölls kan vi konstatera att företagets storlek är den viktigaste faktorn som avgör om en Internetpolicy anses vara nödvändigt eller inte. R1 och R2, som är de två större företagen i vår studie, har en Internerpolicy. R3 och R4, som är de två mindre företagen, har inte utformat en Internetpolicy ännu.

R1 menar att företaget skapat en Internetpolicy för att de inte har något intresse av att bryta mot lagen och inte vill att bolagsnamnet ska förknippas med något som företaget inte står för. Vi anser att detta tyder på en medvetenhet i de konskevenser som kan uppstå om anställda använder Internet på ett felaktigt sätt som inte stämmer överens med företagets värdegrund och intressen. Denna risk blir större ju fler anställda ett företag har och därför blir det naturligt att utforma en Internetpolicy för att minimera de risker som anställdas dator- och Internetanvändning kan medföra. R2, som är det största företaget i vår studie, berättade att det är en självklarhet för ett bolag av deras storlek att ha en Internetpolicy vilket stärker storlekens betydelse.

Både R1 och R2 hade däremot inte utformat ett regelverk för hur anställda skulle förhålla sig till sociala medier, vilket vi tyckte var intressant. Båda företagen var aktiva på sociala medier och hade flera anställda som med största sannolikhet också var aktiva på sociala medier, men hade inga regler/riktlinjer på sådana plattformer. Inledningsvis ansåg vi att detta istället tyder på en omedvetenhet i de effekter som kan skapas av företags närvaro i sociala medier. En intressant anmärkning är dock att R2 numera erkänner att det fanns ett behov av en policy som reglerar anställdas aktivitet på sociala medier eftersom ämnet ”exploderar” som företaget själva beskriver. Det faktum att R2 behöver en policy för sociala medier kan ha orsakats av tidigare incidenter som påverkat företaget och därför anser företaget att det nu behövs ett sådant regelverk. Detta tyder istället på att det skapats en medvetenhet i de effekter som kan skapas av företags närvaro i sociala medier för R2. Enligt Teknikföretagen (2013) kan ett illojalt agerande genom sociala medier vara mycket allvarligare än andra kommunikationsmedel eftersom den potentiella spridningen kan bli enorm. Därför väljer R2 med största sannolikhet att inte ta några risker och väljer därför att utforma en policy som reglerar anställdas användning av sociala medier.

R1 berättade att om anställda vill uttala sig politiskt, rasistiskt eller på något sätt som inte stämmer överens med företagets värdegrund, görs detta som privatperson och inte som anställd. Vi anser att R1 tjänar på att utforma ett regelverk som beskriver hur företagets anställda ska förhålla sig till sociala medier eftersom gränserna mellan arbets- och privatliv

suddas ut. Vi har tidigare beskrivit att arbetstagarens lojalitetsplikt i förhållande till sekretessavtal kan skapa bekymmer eftersom flera arbetsgivare inte vet var gränserna går. Det framgår tydligt att R1 är medveten om vilka konsekvenser som kan uppstå om anställda uppträder på ett sätt som inte är representativt eftersom företaget markerar tydligt att sådant beteende på sociala medier utförs som privatperson och inte som anställd. Ett regelverk syftar inte till att begränsa anställdas användning av sociala medier utan snarare för att ge riktlinjer och rekommendationer för hur anställda ska uppträda och använda sig av verktygen på bästa sätt. Vi anser därför att det är märkligt att R1 inte väljer att utforma en policy för sociala medier, trots att företaget är medvetna om att verksamheten påverkas negativt om anställda uppträder på ett oacceptabelt sätt.

R3 och R4 hade varken en Internetpolicy eller en policy som reglerar anställdas användning av sociala medier, trots att företagen var aktiva på de plattformerna. R3 berättade att företaget var för litet för att en sådan policy skulle behövas, medan R4 inte ens hade tänkt på det. Det framgår tydligt att företagen inte har tillräckligt många anställda för att arbetsgivaren skall oroa sig för anställdas dator- och Internetanvändning eller vad de publicerar på sin fritid.

Vi tyckte det var intressant att veta hur många anställda som krävs för att R4 skulle utforma en Internetpolicy så vi frågade både den dataansvarige och företagets VD. Den dataansvarige som vi först intervjuade svarade att hon redan anser att företaget borde ha en Internetpolicy, medan företagets VD tyckte frågan var intressant men ville inte ge ett svar. Vi anser att det är anmärkningsvärt att företagets VD inte hade ett tydligt svar på frågan när det finns anställda i företaget som anser att ett sådant regelverk borde existera. En Internetpolicy skapas för anställda och är ett viktigt verktyg för att klargöra vad som gäller. Det faktum att den dataansvarige redan tyckte att ett sådant regelverk borde finnas kan vara ett tecken på att anställda inte vet vad som gäller eftersom regler/riktlinjer inte blivit tydligt definierade. Därför kan det finnas en rädsla att skriva och säga vad man egentligen tycker och tänker både på arbetsplatsen och som privatperson. Detta blir också problematiskt för lojalitetsplikten eftersom anställda inte vet hur långt den gäller.

5.2 Dokumentation av Internetpolicy

Om företagen hade en Internetpolicy blev det viktigt för oss att undersöka om den fanns dokumenterad och hur anställda fick ta del av policyn. Detta är viktigt eftersom syftet med Internetpolicyn försvinner om anställda inte får ta del av de regler/riktlinjer som utformats på ett korrekt sätt och detta kommer således att påverka företaget negativt. Eftersom R3 och R4 inte har en Internetpolicy kan en närmare diskussion om dokumentationen inte göras. Därför kommer denna del enbart behandla R1 och R2.

Gemensamt för både R1 och R2 är att Internetpolicyn finns dokumenterad och att anställda får ta del av informationen. Båda företagen behövde en underskrift från den nyanställde i samband med anställningen där de accepterar företagets villkor och skriver under att de inte tänker överträda dessa. Enligt Welebir & Kleiner (2005) är detta det vanligaste sättet att informera anställda om företagets Internetpolicy. Vi anser också att detta är det bästa sättet eftersom företaget tidigt i anställningsprocessen betonar vikten av hur anställda ska uppföra

sig på ett sätt som är representativt för företaget. Om företag är noga med att anställda inte ska bryta regler och liknande måste detta informeras tidigt så anställda förstår innebörden av lojalitetsplikten.

R2 berättade även att samtliga dokument som reglerar hur företaget och anställda ska arbeta, även Internetpolicyn, finns tillgängligt för allmänheten på företagets hemsida, medan detta var något som R1 inte visste om. Detta är ett tydligt tecken på att R2 inte utformat några specifika regler för anställdas dator- och Internetanvändning som de vill dölja. Att företaget öppet publicerar hur anställda ska förhålla sig till webben kan vara ett tecken på att de inte utformat några specifika krav som kan kränka anställdas information- och yttrandefrihet. Vi kan tänka oss att vissa företag skriver tydligt vad anställda får och inte får skriva om företaget för att undvika att bli kritiserade inför allmänheten. Detta kan kränka anställdas yttrandefrihet eftersom grundlagen skyddar anställda att uttrycka sina åsikter om exempelvis arbetsgivaren på sociala medier och detta är något som arbetsgivaren måste respektera.

Vi hittade inga dokument på R1:s hemsida som beskriver hur anställda skulle förhålla sig till Internet, men vi kan fortfarande inte dra några slutsatser för att representanten från R1 inte kunde bekräfta.

5.3 Övervakning & Kontroll

I denna fråga undersökte vi om företagen övervakar eller kontrollerar anställdas dator- och Internetanvändning samt i vilket syfte dessa kontroller görs. Respondenterna skulle även svara om det fanns riktlinjer för hur en sådan kontroll skulle ske, eller om det fanns någon anledning till varför de avstod att övervaka. R1 var det enda företaget som hade någon typ av kontroll medan resterande företag avstod att övervaka fullständigt. Däremot kontrollerade R2 om företagets datorer blivit stulna, men inte vilka hemsidor som besöks eller vad laddas ner.

Enligt R1 sker det ingen kontroll på vad anställda skriver utan företaget kontrollerar vilka hemsidor som besöks och vad som laddas ner. Syftet med kontrollerna grundar sig på anställdas rätt att använda företagets utrustning och därför sker övervakningen enbart på arbetsplatsen. Vi anser att R1 har all rätt att utforma kontroller på företagets utrustning, även om anställda väljer att ta hem utrustningen för privat bruk. I frågan anser R1 att anställda borde förstå att reglerna även gäller utanför kontoret. Däremot medger R1 att företaget inte har några skriftliga dokument på hur en sådan övervakning ska ske, men det framgår i Internetpolicyn att det utförs kontroller på företagets utrustning. Det faktum att det framgår i Internetpolicyn att R1 kontrollerar anställdas användning av företagets utrustning är viktigt. R1 är säkerligen medveten om att lagöverträdelser i samband med övervakning kan resultera i allvarliga sanktioner som inget företag vill utsättas för (IT & Telekomföretagen, 2013). Dessutom har R1 redan betonat att företaget är noga med att inte bryta mot lagen och att bolagsnamnet inte ska förknippas med något som företaget inte står för, vilket stärker det påståendet. De som övervakas måste också bli informerade om ändamålet med övervakningen vilket framkommer i Internetpolicyn.

Trots R2:s storlek och aktivitet på sociala medier sker inga kontroller utöver om företagets datorer blivit stulna och detta reagerade vi på. R2 anser att det är sekretesskränkande att företag går in och övervakar anställdas dator- och Internetanvändning och avstår därför att övervaka helt och hållet. Vi reagerade på detta eftersom det blir allt vanligare att svenska företag kontrollerar anställdas användning av Internet och med tanke på R2:s storlek och position, blev vi överraskade av ett sådant ställningstagande. Däremot kan företaget vara alldeles för stort för att en sådan övervakningspolicy ska vara effektivt. Företaget har flera tusentals anställda och en sådan övervakningskontroll kan vara komplicerad att implementera.

Det faktum att R2 anser att övervakning är direkt sekretesskränkande kan vara ett tecken på att företaget inte vill riskera den problematik som kan uppstå vid databehandling av personuppgifter och liknande. Risken för kränkning av den personliga integriteten innebär att PuL blir aktuellt vilket kan vara något som företaget inte vill behandla över huvud taget. Det faktum att R2 nyligen bestämt sig för att utforma en policy för anställdas användning av sociala medier är ett tecken på att det behövs förändring. Om företaget tydligt markerar hur anställda ska förhålla sig till de sociala verktygen blir behovet av att kontrollera vad anställda skriver inte lika stort.

R3 och R4 berättade att övervakning av anställdas dator- och Internetanvändning inte behövdes. Precis som i frågan om Internetpolicy anser vi att R3 och R4 inte har tillräckligt många anställda för att motivera en övervakningskontroll av denna typ.

5.4 Anställdas dator-och Internetanvändning på arbetstid

Denna fråga syftade till att undersöka om företagen oroade sig för anställdas uppträdande på Internet på arbetstid samt om de gjorde något åt detta. Samtliga företag svarade att de inte oroade sig för anställdas dator- och Interneranvändning på arbetstid.

Enligt R1 är deras anställda så pass högt utbildade och tillräckligt kompetenta i sitt arbete för att förstå vad som får skrivas och vad som inte får skrivas. Däremot medger företaget att det alltid kan finnas någon som missförstått reglerna och som bryter mot dessa medvetet eller omedvetet, men detta är något som företaget inte tänker på. R2 likaså oroade sig inte heller över anställdas aktivitet på nätet, men om anställda skriver olämpliga saker om företagets kunder, måste arbetsgivaren agera.

R2 hade också utformat en uppförandekod, vilket vi tyckte var intressant. R2 var den enda respondenten i undersökningen som hade ett regelverk som beskrev hur företaget skulle bedriva sin verksamhet på ett etiskt, socialt och miljömässigt sätt. Vi förväntade oss inte att R3 och R4 skulle ha något liknande, men vi blev förvånade över att R1 inte hade ett sådant reglerverk. Det faktum att R1 inte oroade sig för anställdas aktivitet på Internet, för att de är tillräckligt kompetenta och utbildade, säger oss att R1 verkligen litar på sina anställda. En intressant fråga man kan ställa sig då är varför R1 är det enda företaget i vår studie som hade ett övervakningssystem. Visserligen kontrollerades endast företagets egna enheter, men utifrån intervjun och de svar som erhölls, är R1 det företag som är mest noggranna med vem som får jobbet. Det känns som att företaget inte behöver kontrollera de hemsidor som besöks

eller vad som laddas ner eftersom de litar på sina anställda så pass mycket. Vi anser inte nödvändigtvis att R1 ljuger i deras förtroende för anställda, men däremot anser vi att det finns en viss oro för anställdas dator-och Internetanvändning som större företag börjar inse. Vi kommer visa ytterligare bevis för detta i anställdas dator- och Internetanvändning på fritid.

R3 och R4 oroade sig inte alls för anställdas dator- och Internetanvändning på arbetstid och hade inte mycket att kommentera i frågan. Precis som vi tidigare konstaterat beror detta med största sannolikhet på företagens storlek. Eftersom R4 kan mäta anställdas resultat blir det uppenbart för ledningen att veta om arbetstimmarna används effektivt eller inte. Upptäcker ledningen i företaget att arbetstimmarna inte används effektivt kommer säkerligen något att göras, men detta hade inte inträffat ännu.

5.5 Anställdas dator- och Internetanvändning på fritid

I denna fråga undersökte vi den syn som företagen hade på anställdas dator- och Internetanvändning på fritid. Vi ville veta om detta bekymrade företagen och om de hade utformat några regler/riktlinjer för anställdas privata hantering av Internet. Gemensamt för samtliga respondenter är att de inte utformat någon sådan policy, men däremot skiljer sig svaren en del gällande om de var lika bekymrade i frågan.

Precis som i frågan om anställdas dator- och Internetanvändning på arbetstid har R1 inte utformat några speciella regler för hur anställda ska uppträda på sin fritid och bekymras inte över detta. Företaget är dock noga med att anställda inte får skada bolagsnamnet, men detta regleras inte och är något som anställda själva förstår. Vi tycker dock fortfarande att det är ganska märkvärdigt att R1 inte bekymras över anställdas Internetanvändning på fritid, men kontrollerar samtidigt regelbundet vilka hemsidor de besöker och vad som laddas ner. Vi anser att sådan kontroll inte borde vara nödvändig om företaget inte bekymras över anställdas surfvanor på sin fritid.

R2 hade inte heller utformat någon policy men erkände däremot att anställdas privata användning av Internet kan vara bekymrande, vilket vi tyckte var intressant. Företaget finns representerade på flera olika sociala medier där tusentals anställda med största sannolikhet också befinner sig, och bekymras över att anställda ska uppträda på ett sätt som kan vara skadligt för bolagsnamnet. Det faktum att R2 nyligen bestämt sig för att skapa en policy som reglerar anställdas användning av sociala medier, stärker påståendet om att företaget bekymras över anställdas aktivitet på sådana plattformer.

Vi anser att det är ganska naturligt att R2 oroas över anställdas dator- och Internetanvändning på fritid med tanke på antalet anställda och den maktposition som företaget har. Vi kan tänka oss att ju mer ett företag vill synas i sociala medier, desto större blir oron för att representanter ska uppträda på ett sätt som kan skada bolagsnamnet. Vi har tidigare nämnt att illojala uttalanden i sociala medier kan få enorm spridning och detta är något som R1 säkerligen är medveten om. Nu uppmärksammar R1 ett behov av att reglera anställdas privata användning av sociala medier för att minimera de risker och hot som kan uppstå. Det hade inte förvånat oss om företaget nyligen upplevt någon kontroversiell händelse på Facebook eller liknande,

där någon anställd uttalat sig på ett sätt som företaget inte accepterade, men detta är enbart spekulationer.

Däremot tyckte vi det är intressant att R2 är det enda företaget i undersökningen som har uppmärksammat ett behov av att reglera anställdas användning av sociala medier. Trots att R1 också är aktiva på flera av de hemsidorna misstänker vi att företaget bekymrar sig mer över utrustningen och att utrustningen inte ska innehålla olämpligt innehåll, som exempelvis en webbhistorik med pornografiska hemsidor. Detta var ett exempel på en kontroversiell händelse som inträffade R1 och som kommer analyseras senare i diskussionen.

Vi misstänkte, med tanke på våra resultat i de tidigare undersökningsområden, att R3 och R4 inte var bekymrade över anställdas privata hantering av Internet och så var fallet. Vi berättade för R4:s VD att felaktig hantering av Internet från anställda innebär mycket mer än att de privatsurfar ett par minuter, utan det kan handla om olämpliga och illojala uttalanden som kan få enorma konsekvenser. I den frågan svarade VD:n:

”*Egentligen handlar det mycket om att rekrytera rätt tänker jag. Om någon vill skada företaget kan man aldrig 100% skydda. Det finns inte resurser och tid för att lägga upp system inom företaget för att kolla sånt på sociala medier och liknande när vi är ett mindre företag.”* (Bilaga B4, s.60).

Det uttalandet bekräftar ännu en gång att företagets storlek är en betydande faktor i hur arbetsgivaren och företaget ska förhålla sig till anställdas privata dator- och Internetanvändning. Baserat på intervjuerna anser vi att mindre företag fokuserar mer på att rekrytera rätt medarbetare och därmed försäkrar sig om att den personen inte bara gör ett bra jobb, utan också uppför sig privat. När företag börjar rekrytera ett stort antal personer som kommer från olika erfarenhets- och utbildningsbakgrunder, kommer det synas att surfvanor och privat användning av Internet kraftigt varierar. R2 är det närmaste företaget i vår undersökning som speglar den verkligheten och med tanke på att R2 är det enda företaget som börjat uppmärksamma bekymmer i denna fråga, stärker det vårt påstående.

En annan intressant anmärkning som kan tas från uttalandet är att företag ändå aldrig kan till 100% skydda sin verksamhet från en anställd som har bestämt sig för att skada. Vi håller med om detta och tänker oss exempelvis om någon har bestämt att uttala sig extrempolitiskt på Facebook, då finns det inte mycket företaget kan göra åt detta. Då handlar det mer om, precis som R4 sade, att rekrytera rätt. En intressant strategi som större företag borde tillämpa är att tidigt i anställningsprocessen försäkra sig om att den nyanställde inte uppträder på ett olämpligt sätt online. Det kan handla om att ställa personliga frågor som berör personens privata användning av Internet, istället för att enbart ge företagets syn i frågan genom Internetpolicyn.

5.6 BYOD

I frågan om BYOD undersökte vi företagens syn på anställdas personliga utrustning samt vilka för- och nackdelar de kunde identifiera med BYOD. Gemensamt för samtliga företag är att de tillåter anställda att tag med sig sin personliga utrustning till arbetsplatsen, men i frågan om de får koppla upp sig mot företagets nätverk, skiljer sig svaren en del.

R1 berättade att anställda får tag med sig sin personliga utrustning till arbetsplatsen, men tillåts inte koppla upp utrustningen till företagets nätverk eller server. Denna BYOD-policy har företaget utformat på grund av de sekretessavtal som skrivits på med kunder som innebär att tjänsteinformation inte får spridas till obehöriga, och detta tar R1 på fullaste allvar. De riktlinjer som företaget har gällande BYOD finns reglerade i företagets Internetpolicy.

Vi har tidigare i litteraturgenomgången beskrivit att sammanblandning av tjänsteinformation och privat information är en utmaning som finns i BYOD. Det uppstår en problematik när anställdas integritet ställs emot arbetsgivarens kontroller. Arbetsgivaren måste då fråga sig om det finns tekniska, juridiska och praktiska förutsättningar att genomföra kontroller på den privata utrustningen som används i tjänsten. Trots att R1 kontrollerade anställdas privata hantering av Internet, som exempelvis vad som laddades ner, kan denna problematik inte fullständigt appliceras på R1 eftersom anställda använder sig av företagets utrustning för privat bruk, inte sin egen. Det faktum att anställda använder utrustningen för privat bruk och sedan kopplar upp sig mot företagets nätverk, förändrar ingenting eftersom utrustnigen fortfarande är R1:s egendom. Därför har R1 all rätt att kontrollera anställdas dator- och Internetanvändning eftersom utrustningen är en del av företagets, som vi tidigare beskrivit och håller med om. Däremot ifrågasatte vi företagets förtroende för anställdas privata hantering av Internet eftersom de hela tiden betonade att anställda är tillräckligt utbildade och kompetenta, men samtidigt kontrollerade regelbundet vad anställda gör med utrustningen privat. Om företagets anställda hade fått tillåtelse att koppla upp sin personliga utrustning mot nätverket, hade situationen blivit intressant eftersom då ställs särskilda krav på noggrannhet och tekniska begräsningar av olika slag för att information inte ska sammanblandas. I detta fall står, underhåller och äger R1 utrustningen och därför får de göra vad de vill.

R2 började sitt svar med att förklara att BYOD är en ”het grej” idag och att det finns utmaningar att hantera. R2 berättade att anställda får tag med sig sin personliga utrustning till arbetsplatsen, men föredrar att de använder företagets enheter eftersom dessa enbart får kopplas mot nätverket, precis som R1. R2 hade också en BYOD-policy där samtliga regler/riktlinjer finns för anställdas personliga utrustning.

Anledningen till varför endast företagets enheter fick kopplas mot nätverket var de särskilda säkerhetsprogram som var installerade. Om utrustningen skulle blivit stulen kunde företaget enkelt utföra en blockeringsfunktion som gjorde utrustningen funktionsoduglig och dessa säkerhetsprogram var inte installerade på anställdas privata utrustning. Detta var inte förvånande för oss att höra eftersom säkerhetsriskerna är det tyngsta motargumentet mot BYOD, som vi tidigare i litteraturgenomgången beskrivit. Undersökningen från Dimensional Research (2012) beskrev anställdas brist på säkerhetsmedvetenhet som det största hotet mot

företagsdata och detta är ett tydligt exempel varför. R2 fokuserade enbart på säkerhetsriskerna i frågan och oroades över utrustningens sårbarhet. Med tanke på antalet anställda som företaget har, hade det varit extremt svårt att kontrollera samtliga enheter som kopplas mot företagets nätverk och därför tillåter inte R1 att anställda gör detta med sin privata utrustning.

R3 och R4 såg inga problem med att anställda tar med sig sin personliga utrustning till arbetsplatsen och dessutom kopplar utrustningen mot företagens nätverk. Båda företagen hade inte utformat någon BYOD-policy utan användningen av anställdas personliga enheter var relativt fritt. R3 berättade i frågan att de enbart ser fördelar om anställda har de enheter som de är vana vid att använda och den utrustning som de själva vill ha. Vi anser, ännu en gång, att detta direkt kopplas till företagens storlek.

5.7 Tidigare incidenter

I frågan om tidigare incidenter undersökte vi om företagen påverkats av någon tidigare händelse där anställdas privata dator- och Internetanvändning på något sätt skapat problem för företaget. Vi ville veta hur företaget påverkades av händelsen samt om det skedde några förändringar efteråt. Vi har kommit fram till att varje incident som inträffat har påverkat respondenterna på något sätt och resultera i någon form av åtgärd från ledningen. Däremot hade R3 och R4 inte upplevt någon tidigare incident som orsakats av anställdas privata dator- och Internetanvändning, men det hade R1 och R2.

Som tidigare beskrivits hade R1 blivit kontaktade av polisen för att någon anställd hade via deras personalnätverk behandlat pornografiska hemsidor och detta var något som ledingen i företaget inte visste om. I frågan om hur företaget påverkades av händelsen säger R1 att utåt förändrades inte särskilt mycket eftersom det endast var ett fåtal personer som kände till incidenten, men internt fick företaget upp övervakningsfrågan på agendan och började blockerade vissa typer av hemsidor. Vi kan alltså konstatera att R1 påverkades väldigt negativt av incidenten eftersom företaget tidigare inte kontrollerat anställdas användning av Internet, men nu uppmärksammades frågan och gick igenom. Vi anser att medvetenheten i anställdas privata och yrkesverksamma dator- och Internetanvändning blev större och därför beslutade R1 att inte längre ta några risker och utformade därmed ett övervakningssystem för dess anställda. Detta påverkade företagets BYOD-policy och gjorde den mer strikt.

R2 berättade att företaget säkerligen varit involverade i flera incidenter som berör anställdas användning av Internet eftersom företaget hade tusentals anställda och var verksamma i flera länder. De senaste åren hade flera datorer blivit stulna vilket påverkade företaget enormt, men däremot ville R2 inte diskutera vilka åtgärder som utfördes efter incidenterna. Vi tror att företaget installerade särskilda säkerhetsprogram som ett resultat av antalet bestulna datorer, och inte ville diskutera ytterligare åtgärder eftersom de förmodligen involverade personliga konsekvenserför de anställda som var ansvariga. Det faktum att R2 inte ville diskutera vilka åtgärder som utfördes bekräftar att företaget påverkades negativt av händelsen och gjorde företaget mer medveten om de negativa effekterna av anställdas privata och yrkesverksamma dator- och Internetanvändning.

6 Slutsats

I detta kapitel redovisar vi de viktigaste slutsatserna i vår undersökning.

I uppsatsens inledning ställde vi oss frågan:

- *Hur påverkas företag av anställdas privata och yrkesverksamma dator-och Internetanvändning?*

För att besvara denna fråga har vi bestämt oss att dela in svaret i två delar. Den första delen behandlar hur större företag påverkades och den andra delen behandlar hur mindre företag påverkades. Detta gjorde vi eftersom den viktigaste faktorn som avgjorde på vilket sätt företag påverkades av anställdas privata och yrkesverksamma dator- och Internetanvändning var företagets storlek. Vi har kommit fram till, baserat på vårt undersökningsmaterial, att större och mindre företag inte påverkades på samma sätt och därför behandlas vardera separat. (se kapitel 4.8)

Genom att analysera undersökningen resultat har vi kommit fram till att större företag är mer försiktiga och medvetna i frågan eftersom det är en större sannolikhet att de reglerar och kontrollerar anställdas privata och yrkesverksamma dator- och Internetanvändning. Eftersom större företag är mer medvetna om de negativa effekterna av anställdas användning av sociala medier och BYOD, måste företagen skapa tydliga policys och i vissa fall även övervaka för att undvika de risker och hot som kan uppstå. I samband med detta är det vanligare att större företag upplevt tidigare incidenter som påverkat verksamheten på ett negativt sätt och resulterat i någon form av åtgärd från ledningen.

I frågan om hur mindre företag påverkas har vi kommit fram till att de är mer positivt inställda till anställdas privata och yrkesverksamma dator- och Internetanvändning och inte kände ett behov av att anpassa företaget efter anställdas användning av sociala medier och BYOD. Mindre företag bekymras inte på samma sätt som större företag eftersom de negativa effekterna inte anses vara tillräckligt allvarliga och sannolika att inträffa. Företagen påverkas inte av anställdas privata användning av Internet på arbetsplatsen, vilket gör företagen mer positiva till de fördelar och möjligheter som sociala medier och BYOD medför.

Bilagor

B1 – Transkribering 1

Intervjuperson: Hej!

Intervjuare: Hej, det är vi som skulle intervjua dig.

Intervjuperson: Hej hej!

Intervjuare: Är du redo för att köra igång?

Intervjuperson: Ja, det är bara att köra på.

Intervjuare: Då kör vi, det är så att vi skriver vår kandidatuppsats om anställdas Internetanvändning och surfvanor. Vi försöker fördjupa oss om hur anställda jobbar med sin utrustning och hur de surfar på arbetsplatsen samt privat med exempelvis sociala medier och liknande.

Intervjuperson: Ja.

Intervjuare: Ni är ett företag som har anställda?

Intervjuperson: Absolut.

Intervjuare: Den första frågan är då, finns det regler för den anställdes Internetanvändning? Exempelvis vad de skriver på sociala medier och liknande?

Intervjuperson: Ja, vi har ett regelverk för hur vi får använda våra resurser och hur vi får agera när vi är ute på nätet. Men vi har inte något regelverk som beskriver vad vi får skriva och vad vi inte får skriva. Utan det som vi har generaliserat det till, är att man inte får befinna sig i aktiviteter eller platser som är olagliga eller oetiska.

Intervjuare: Ja, hur tänkte ni då ni bestämde reglerna?

Intervjuperson: Hur vi tänkte?

Intervjuare: Ja, hur ni satte upp reglerna?

Intervjuperson: Ja, det är ganska enkelt. Vi har inte något intresse att bryta mot lagen som företag eller någon medarbetare, detta är väldigt klockrent.
Vi har även väldigt svårt att förstå att anställda eventuellt skulle göra uttalande eller engagera sig i olagligheter eller på något sätt ha en sådan bakgrund i bolaget. Vi vill inte att vårt bolagsnamn ska förknippas med något sådant eller stå i strid med något som bolaget inte vill. Vi anser inte att man får använda vår utrustning och vårt företags namn i sammanhang som inte strider för företagets grundvärderingar och normer som finns.
Det är väl det, men om någon enskild person vill begå brott eller uttala sig politiskt, rasistiskt eller på något annat sätt. Då får man göra detta som privatperson, inte på något sätt förknippa sig med företaget.

Intervjuare: Ok, finns de här reglerna dokumenterade?

Intervjuperson: Ja, de finns dokumenterade i vårt kvalitéts ledningssystem som är certifierade. Där har vi vår policy och våra styrdokument som styr hur vi får arbeta och vad vi tar för åtagande på oss. När någon börjar hos oss får de skriva på någon liten blankett där alla regler och förhållningsreglerna finns nertecknade. Då tar de på sig hur de får arbeta och godkänner vår företags policy och vi försäkrar oss att de lever upp till vår policydokument och inte överträder dessa.

Intervjuare: Ok, vår nästa fråga är då. Får den anställde informationen om reglerna? Hur får den anställde reda på reglerna? Detta är då att den anställde skulle skriva på i början av anställningen som du sa eller?

Intervjuperson: I samband med att den anställde skriver på ett anställningsavtal så behöver de skriva på den här blanketten vilket försäkrar att de har läst på policy avtalen, samt hantering av vår utrustning, kommunikationen utåt och dessa sparar företaget. Denna information får de vid anställningen och i vårt introduktionsmöte, vilket sker första veckan av anställningen. Där får den anställda klart och tydligt se vilka regler som gäller och hur de använder sig av utrustningen. Det blir som en liten introduktion och uppfräschning av det som de redan har förbundit sig att leva efter.

Intervjuare: Ja det låter bra, nästa fråga. Sker det någon kontroll av den anställdes Internetanvändning?

Intervjuperson: Vi kontrollerar inte vad de skriver. Men vi har kontroll på vilka sidor de besöker och vad som laddas ner, detta finns i vår Internetpolicy. Vi har någon gång gjort några påkallade kontroller på någon specifikt medarbetare, i samband då att vi har upptäckt att någonting inte riktigt är som det borde. Då har vi analyserat och kommit fram till att det har varit aktiviterat med någon anställd som inte då har hållit till dessa regler de har skrivit på. Så det har skett, men vi gör inte någon kontinuerlig stickprovs kontroll.

Intervjuare: De här kontrollerna, samt att ni har koll på vilka sidor de besöker och vad de laddar ner. Sker detta även privat eller bara på arbetsplatsen?

Intervjuperson: Nej, det sker enbart på arbetsplatsen. Vi har inte någon övervakning över folks vardagliga rutiner. Men om de plockar med sig företags utrustning så kan vi alltid kontrollera dessa. Så användning av vår utrustning gäller även om man är hemma. Det är inte den enskildes egendom utan bolagets egendom, och då hoppas vi att de har fantasi nog att förstå att reglerna gäller även om de inte är inne på kontoret. Däremot har vi alltid möjlighet att se om någonting inte har hanterats på vårt sätt. Detta kan ske exempelvis när vi ska göra en uppdatering, byta filer eller helt enkelt när någon slutar och vi får tillbaka utrustningen. Då kan vi se saker som skett utanför arbetstid eller på företagets nätverk, men som sagt ingen kontroll sker slumpmässigt.

Intervjuare: Ok, då blir nästa fråga väldigt passande. Oroar ni er för att era anställda ska göra bort sig på nätet?

Intervjuperson: Nej, det gör vi faktiskt inte för vi anser att våra anställda är så högt utbildade och kompetenta i sin profession att de ska veta vad de får och inte får göra. Vi anser att de som arbetar hos oss vill nog jobba för oss och att våra regler är så självklara att detta inte behövs. Så nej, men det finns alltid någon som kan ha missförstått detta och bryter mot något medvetet eller omedvetet, men det är inget vi oroar oss för särskilt mycket.

Intervjuare: Kan det vara så att när den ny anställde skriver på avtalet i början så förutsätter ni kanske i början att de här inte ska ske, utan ni liter på den personen.

Intervjuperson: Det finns väldigt mycket i samspelet mellan den enskilde medarbetaren och företaget som bygger på ett ömsesidigt förtroende. Jag har nog väldigt svårt att tänka att vi inte har något förtroende för de som vi anställer och arbetar med. Jag har väldigt svårt att förstå att vårt samarbete, vår relation mellan företag och medarbetar inte kan bygga på ömsesidig förtroende. Den dagen jag inte litar på någon medarbetare, då kommer jag att ta till aktiviteter som göra att bolaget och medarbetaren skiljs med varandra. För det fungerar inte med oss lika mycket som med någon annan, att man inte har något förtroende för varandra och litar på varandra. Så det korta svaret är, ja.

Intervjuare: Hur känner ni om anställdas surfvanor på sin fritid? Är det något som bekymrar er? Har ni regler för hur anställda ska bete sig på sin fritid ute på nätet? Händer det att era medarbetare på fritiden direkt eller indirekt representerar sin arbetsgivare eller företaget?

Intervjuperson: Nej, det har vi inte. Vi har inte några direkta regler om hur anställda ska bete sig på sin fritid. Förutom kanske om de gör andra aktiviteter som exempelvis bär en företags tröja eller om de kör en av våra företags bilar privat. Även då förutsätter vi att de inte bryter mot reglerna eller beter sig på något sätt som påverkar vårt företags namn negativt. Detta gäller även för anställdas datoranvändning och liknande.

Intervjuare: Vad tycker ni om anställdas egna tekniska utrustning? Finns det några problem som ni ser? Ser ni några fördelar?

Intervjuperson: Ja, om vi säger så här. Man får ta med sig sin utrustning till arbetsplatsen, men de får inte koppla in den mot vår server, vårt nätverk eller någon annan utrustning. De får gärna ta med sig och ha det som en ”stand alone device”. Men vi är väldigt reflektiva med den utrustning vi behöver i vårt arbete eller internt för att arbeta hos oss, gäller även den utrustning vi behöver när vi ska jobba ut mot kunden. Vilket är vårt primära syfte, att arbeta i skärpa kund uppdrag. Den utrustningen står bolaget för, den äger bolaget, den underhåller bolaget.

Intervjuare: Finns det någon anledning om varför man inte får använda företagets nätverk?

Intervjuperson: Ja, en jätte viktig anledning. Det är för att vi har kraftig sekretess ut mot obehöriga, även personer som kan bli obehöriga för utrustingen som kopplas in. Vi har specifika sekretessavtal med våra kunder som innebär att vår information inte får spridas till annat än behöriga, våra lokaler får inte trädas av obehöriga. Sen kan det vara väldigt olika beroende på vad det är för kund och vilket avtal vi skrivit på.

Intervjuare: Ja ok, då kommer vi till sista frågan. Finns det exempel på tidigare händelser där anställdas Internetanvändning har skapat problem för företaget?

Intervjuperson: Någon gång hade vi en kontroll mellan tre bolag, ett moderbolag och två dotterbolag. Där vårt företag var inblandat, vilket nu mera har en helt annan ägarbild än vad vi har och som vi har sålt av för två år sedan. Men i vilket fall som helst hade vi ett samröre i ett gemensamt projekt som hade med utbildningar att göra. Det rörde sig om många olika utbildningar inom gymnasier, arbetsmarknadsutbildningar, högskoleutbildningar och skräddarsydda företags utbildningar kan man väl säga. På den tiden så hade man ett stort nätverk på respektive ort man var verksam på och man hade ett personalnätverk som var separat från varandra. Där hade vi någon form av incident som vi faktiskt inte vet vad det är till hundra procent. Vi blev kontaktade av polisen för att det hade varit någon ingång från ett av våra nätverk som behandlade pornografi. Vi fick då samarbeta med polisen för att ta reda på var någonstans man har besökt dessa sidor. Det visade sig att en anställd hade varit inne där, men vad som föll ut av det vet jag faktiskt inte mycket om. Jag tror att på någon sätt redde de ut situationen och hitta någon form av lösning utan rättsliga eller polisära åtgärder. Det var en konstigt incident när vi blev uppringda, först var vi inte heller medvetna om var någonstans man hade suttit och tagit sig in på sidor som var så oerhört uppstyrda från vår sida. Så ja, detta har hänt.

Intervjuare: Oj ja. Hur påverkades företaget av incidenten? Skedde det några förändringar eller liknande efteråt?

Intervjuperson: Jag skulle vilja påstå att utåt förändrades det inte särskilt mycket eftersom det bara var ett fåtal personer som kände till incidenten. Det var vår nätverksansvarig, den enskilde anställda och någon till som var involverade i händelsen. Internt så stramade vi upp övervaknings situationen på vårt personalnätverk samt elevnätverk och vi stängde rätt mycket portar både in och ut. Men på den tiden så var det inte lika stora möjligheter att blockera och stänga sidor som det är idag. Så ja, det påverkade oss självklart.

Intervjuare: Ok, det var alla frågor. Tack så mycket. Skulle du och ditt företag vilja vara anonyma eller går det bra att använda oss av era namn?

Intervjuperson: Hur ska uppsatsen sammanfattas, presenteras och vad är det som kommer att komma ut?

Intervjuare: Det är vår kandidatuppsats. Så det här är vår empiriska undersökning. Vi måste fråga om ni vill vara anonyma eller inte. Vi behöver inte nämna namn eller liknande om ni inte vill men vi kommer att använda oss utav frågorna och svaren vi fått av er idag. Det är en väldigt viktigt och central del av uppsatsen och något som lärarna måste kunna kolla på.

Intervjuperson: Ja ok. Då tror jag faktiskt att vi vill vara anonyma med våra namn. Men ni får hemskt gärna skriva att vårt företag är ett medelstort IT bolag inom elektronik utveckling och inbyggda system.

Intervjuare: Ja absolut. Det är ingen fara, det är väldigt ofta företag väljer att vara anonyma. Då skriver vi att ni vill vara anonyma. Har ni några avslutande tankar eller kommentarer?

Intervjuperson: Nej, det har jag väl inte. Men det hade varit hemskt roligt att få ett exemplar av er kandidatuppsats så att jag kan se lite grann vad ni kom fram till för resultat samt lära mig lite av den.

Intervjuare: Ja absolut. Vi har din mail och kommer att skicka det till dig slutet av nästa månad.

Intervjuperson: Ja det får ni jätte gärna göra, absolut.

Intervjuare: Då tackar vi dig jätte mycket för att ni har ställt upp med vår intervju. Vi vill också tacka dig för att du gav väldigt utförliga svar, det uppskattas väldigt mycket. Vi önskar dig en god fortsättning.

Intervjuperson: Tusen tack själva. Jag tycker det var väldigt bra genomarbetade frågor och intressanta frågor att reflektera över. Jag hoppas att ni får ihop någon bra uppsats som hjälper er med utbildningen och självklart en god fortsättning.

Intervjuare: Tack så mycket!

Intervjuperson: Jag ser fram emot rapporten.

Intervjuare: Ja då, tack återigen.

Intervjuperson: Ingen fara, hej hej!

Intervjuare: Tack, hej då!

B2 – Transkribering 2

Intervjuperson: (Började med sitt namn.)

Intervjuare: Hej.

Intervjuperson: Hallå, ja.

Intervjuare: Det är vi som bestämde att göra en intervju nu.

Intervjuperson: Ja, det stämmer. Stämmer bra. Väldigt punktlig var ni.

Intervjuare: Ja, är du redo för intervjun?

Intervjuperson: Ja. Hörs det bra?

Intervjuare: Ja då, det hörs bra. Ok, då hade vi tänkt intervjua dig om anställdas dator- och Internetanvändning. Den första frågan är: Har ni i ert företag några regler för anställdas dator- och Internetanvändning. Exempelvis vad han eller hon får skriva på sociala medier.

Intervjuperson: Ja. Den är lite svår, vi håller på att jobba lite med det just nu ska jag säga er, den policy frågan.

Intervjuare: Ok.

Intervjuperson: Vi har interna sociala medier och liknande, som exempelvis bloggar. Externt har vi inte utfört någon policy. Utan där gäller det nog bara sunt förnuft.

intervjuare: Ok. Finns det någon anledning till varför ni gör det nu eller tog det lång tid att sätt upp regler?

Intervjuperson: Nej, det är att det explodera. Det är väldigt mycket snack med sina kollegor. Sen börjar vi prata om till exempel incidenter och allt till arbetslivet som inte får eller ska komma ut utanför företaget. Det kan vara rent interna saker som inte kompisar eller obehöriga ska se egentligen. Det är därför vi tittar mer på det just nu.

Intervjuare: Ok. Sker det någon kontroll av era anställdas dator- och Internetanvändning i företaget? Kontrollerar ni vad de skriver?

Intervjuperson: Nej, inte på vad dem skriver. Nej det gör vi inte. Vi har kontroll på datorerna i säg om de till exempel blir stulna. Men inte vad de skriver på sociala medier.

Intervjuare: Ok. Finns det regler eller riktlinjer efter hur den kontrollen sker?

Intervjuperson: Nej, det finns inte någon sådan kontroll.

Intervjuare: Ok.

Intervjuperson: Inte vad man skriver. Nej, det är sekretesskränkande att företaget går in och tittar på vad anställda skriver på sociala medier och liknande.

Intervjuare: Det jag menar är liksom om den här kontrollen som ni gör av anställdas dator- och Internetanvändning. Finns den dokumenterad? Kan anställda se att ni gör det?

Intervjuperson: Vi gör inte det sa jag.

Intervjuare: Aha ok. Oroar ni er för att era anställda ska göra bort sig på nätet? Samt gör ni något åt detta?

Intervjuperson: En gång till, det blev lite dåligt ljud.

Intervjuare: Ok, oroar ni er för att era anställda ska göra bort sig på nätet? Samt gör ni något åt detta?

Intervjuperson: Göra bort sig?

Intervjuare: Ja. Exempelvis skriver olämpliga saker?

Intervjuperson: Du menar på sociala medier. Nej, det är privat. Om de gör det på sociala medier så är det privatagerande som de gör. Inget som vi kontrollerar, utan det är bara om de uttrycker sig om våra kunder. Eller om man uttrycker någonting om företaget och de sprider sig på något informellt sätt så att vi som arbetsgivare får kännedom av det, då får vi agera. Men vi har inget regelverk som hanterar det.

Intervjuare: Ok.

Intervjuperson: Vi har något som heter Code of Conduct, som beskriver hur anställda ska agera och hur de ska uppföra sig mot ens kunder eller leverantörer. Det regelverket gäller och detta har alla anställda skrivit på, vilket regler som gäller. Allt detta finns på vår hemsida och alla anställda måste läsa igenom informationen, samt skriva på att de måste följa reglerna när vi anställer dem.

Intervjuare: Hur känner ni om anställdas surfvanor och Internetanvändning på deras fritid? Är det något som bekymrar er?

Intervjuperson: Vi finns på flera sociala medier och vet att våra anställda också finns där. Ibland tänker vi på vad de skriver och liknande om företaget och sånt. Vi kommer inom en snar framtid att förhoppningsvis släppa hur vi vill att anställda ska uppföra sig på sociala medier.

Intervjuare: Ok. Vad tycker ni om anställdas egna tekniska utrustning? Får de ta med sig sin egna utrustning till arbetet?

Intervjuperson: Detta är en het grej idag. Många har surfplattor och datorer som företaget oftast står för. Då försöker vi ordna så att de kan säkert använda sin utrustning och ser till så att de är skyddade. Blir exempelvis utrustningen stulen så ska den som stjäl inte kunna leta och hitta företagets information. Vi föredrar dock att anställda använder vår utrustning.

Intervjuare: Ok. Ser ni några problem med att anställda tar med sin egen utrustning?

Intervjuperson: Det är en liten utmaning att hantera.

Intervjuare: Ja.

Intervjuperson: Det är ingenting vi stoppar utan det för de göra. Utan då är det begränsad återkomst. Det kommer inte åt insidan av nätverket utan det är det som i så fall är publicerat ute på Internet de kommer åt.

Intervjuare: Ja ok. Sista fråga då. Finns det exempel på tidigare händelser på ert företag där era anställdas dator- och Internetanvändning har på något sätt skapat problem? Jag vill bara påminna dig om att denna intervju kan vara helt anonym om du vill det.

Intervjuperson: Ja det är nog bra om detta är anonymt.

Intervjuare: Du vill vara anonym eller?

Intervjuperson: Ja, det blir nog bra.

Intervjuare: Ok, absolut!

Intervjuperson: Ja, vi är ett stort företag men nästan 10 000 anställda. Så det har säkert förekommit flera incidenter.

Intervjuare: Kan du komma på något exempel?

Intervjuperson: Ja.

Intervjuare: Finns det kanske någonting om sociala medier som har blivit fel där?

Intervjuperson: Ja, vi har haft en driftstörning som har drabbat. Eller nej, där hände ingenting. Den typen av incidenter har sig en liten grupp som inte ska ut på något intranät som ska informeras direkt. Så jag har inte något bra exempel just nu.

Intervjuare: Ok.

Intervjuperson: Däremot har datorer blivit stulna, vilket är väldigt allvarligt. Att företag slarvar med sin utrustning, då har anställda inte följt nått exempel på policyn. Då måste det vara så att en programvara ska vara installerat mot stöldskydd. Då kan vi blockera utrustningen när den hamnar i obehöriga händer och helt enkelt gör dem funktionsoduglig. Det har hänt att en utrustning har blivit stulen och programvaran inte varit installerad. Det känner jag till. Jag vill inte gå in på vad vi gjorde för att åtgärda problemet.

Intervjuare: Ok. En liten fråga till bara? Ni har en Internetpolicy? Eller missuppfatta vi dig där?

Intervjuperson: Ja, vi har Internetpolicy men om sociala medier har vi inte skrivit någon policy om. Vi arbetar lite på den just nu.

Intervjuare: Men ni har en Internetpolicy allmänt i företaget eller?

Intervjuperson: Ja, det har vi.

Intervjuare: Ok. Hur tänkte ni när ni satte upp reglerna?

Intervjuperson: Det är ganska självklart för ett bolag av vår storlek och position att ha en sådan policy.

Intervjuare: Ok. Då var det intervjun och vi vill båda två tacka dig för att du medverka. Och som vi har förstått det så vill du vara anonym?

Intervjuperson: Ja det vill jag helst.

Intervjuare: Ok. Det fixar vi, ingen fara! Då tackar vi hemskt mycket för din tid.

Intervjuperson: Ja, tack själva! Lycka till!

Intervjuare: Tack ska du ha. Ha det bra! Hej då!

Intervjuperson: Detsamma, Hej då.

B3 – Transkribering 3

Intervjuperson: Ja, hej!

Intervjuare: Hej, du minns att vi hade en intervju idag?

Intervjuperson: Ja, just det. Det var nu, ja!

Intervjuare: Ja precis.

Intervjuperson: Ja, men kör på!

Intervjuare: Vill bara säga att du kan vara helt anonym i intervjun om du vill. För dem vi har intervjuat tidigare märker vi att de inte har varit lika ärliga, för de trodde vi publicera allting.

Intervjuperson: Ja, men det blir nog bra.

Intervjuare: Ok. Den första frågan är om ni har några regler eller någon typ av Internetpolicy för era anställdas dator och Internetanvändning?

Intervjuperson: Nej, det har vi inte. Vi har inget nerskrivet.

Intervjuare: Ni har inte det eller?

Intervjuperson: Nej.

Intervjuare: Hur tänkte ni då när ni inte bestämde några regler?

Intervjuperson: Nej men asså, vi är fortfarande ett litet företag och jobbar i ett kontor tillsammans. Alla har sina egna datorer som de arbetar ifrån. Vi liter på den goda vilja och sunt förnuft.

Intervjuare: Hur många anställda är ni?

Intervjuperson: Vi är åtta stycken.

Intervjuare: Aha, Ok. Då förmodar vi att ni inte kontrollerar varandra om vad ni skriver, asså det sker inte någon form av kontroll av anställdas dator- och Internetanvändning?

Intervjuperson: Nej, det har vi inte. Det behövs inte för vårt företag, det skulle inte hjälpa oss.

Intervjuare: Ni oroar er inte heller för att era anställda ska göra bort sig på nätet eller något liknande? Skriva olämpliga saker.

Intervjuperson: Nej, det gör vi inte. Det är ungefär fem personer som är aktiva på Twitter, Facebook och liknande och dem litar vi i stort sätt på.

Intervjuare: Ok, och ni har inga riktlinjer eller liknande?

Intervjuperson: Nej, inget nerskrivet.

Intervjuare: Ok. Vi måste bara fråga i framtiden, om ni får flera anställda samt företaget växer. Kan det bli aktuellt att ni skaffar en solid Internetpolicy, riktlinjer och liknande för hur anställda ska förhålla sig till sociala medier och liknande?

Intervjuperson: Jo, det kan jag tänka mig om vi blir riktigt stora.

Intervjuare: Men det är inget som ni behöver nu?

Intervjuperson: Nej då. Just nu känns det ok att sitta och skriva dokument. Vi pratar liksom om hur vi ska exempelvis marknadsföra oss på Internet, vad vi ska kommunicera för något samt vad är det är för produkt vi ska trycka på och liknande.

Intervjuare: Ja ok. Dina kollegor, hur känner du för deras surfvanor på sin fritid? Är det något som bekymrar dig? Har ni regler för hur de ska uppföra sig på nätet? Alltså på sin fritid inte på arbetsplatsen.

Intervjuperson: Det bryr vi oss inte om överhuvudtaget just nu. Vi har inte haft någon tanke om det heller.

Intervjuare: Ok. Vi förmodar att ni tar med er egen utrustning till arbetsplatsen då?

Intervjuperson: Ja, det gör vi. Vi har våra egna datorer som vi köra på.

Intervjuare: Ok. Har det skett några problem med det?

Intervjuperson: Nej, det har det inte. Det är bara fördel att folk har dem datorerna som de är vana vid att använda och som de själva vill arbeta med.

Intervjuare: Ja, precis. Du ser bara fördelar med det alltså?

Intervjuperson: Ja.

Intervjuare: Ok. Vi kan testa med denna fråga också. Finns det exempel på något som har hänt tidigare där det har blivit några problem med dator- och Internetanvändning eller liknande? Har det liksom hänt något med era datorer eller på nätet där ni har tänkte att detta inte var bra?

Intervjuperson: Nej, inte på något sätt som vi själva eller någon anställd har gjort.

Intervjuare: Har du kanske jobbat för ett annat företag tidigare som det har hänt något sådant?

Intervjuperson: Nej, det har jag inte.

Intervjuare. Nej, ok. Det fick bli en liten snabb intervju för vi visst inte riktigt ni var åtta anställda. Men vi tror ändå att vi kan skriva någonting om detta här, vi ska också analyser mindre företag.

Intervjuperson: Ja, precis. Detta är ett bra exempel på någon liten start, liksom lita på den enskilda.

Intervjuare: Ja, precis. Men du tyckte och var överens om att när ni blir större så blir det lämpligt att skaffa sig en Internetpolicy eller liknande?

Intervjuperson: Det som jag tänker mig är att med sociala medier och liknande, så handlar det om någon brandin guideline. Hur vill vi egentligen uppfattas utåt, hur ska vi formulera? Ska vi råsälja? Att vi sätter rätt ton i dialogen med kunderna. Då kan jag tänka mig att det blir en del av brandbooking.

Intervjuare: Ja, vi tror inte vi har mycket mer än detta om det inte är något du vill säga eller kommentera?

Intervjuperson: Nej, inget jag kommer på nu.

Intervjuare: Ok, då tackar vi för din tid och önskar dig en fortsatt trevlig dag.

Intervjuperson: Det var så lite så, tack själva och lycka till!

Intervjuare: Tack, hej hej!

Intervjuperson: Hej hej!

B4 – Transkribering 4

Intervjuperson: Hej!

Intervjuare: Hej! Tack för att vi fick komma.

Intervjuperson: Ingen fara, det är bara trevligt. Men VD:n kan inte komma just nu så ni får intervjua mig så länge om det går bra?

Intervjuare: Ja, det går jättebra, tack.

Intervjuperson: Då går vi in i detta rum. Om det är något ni behöver så säga till.

Intervjuare: Nej, tack! Ska vi köra igång?

Intervjuperson: Ja då.

Intervjuare: Ok. Första frågan är då, om ni har regler för era anställdas dator- och Internetanvändning? Om ni har en Internetpolicy? Exempelvis vad anställda får skriva på sociala medier.

Intervjuperson: Vi har inga skriftliga regler.

Intervjuare: Ok, hur tänkte ni då?

Intervjuperson: Ingen som riktigt har tänkt på det.

Intervjuare: Ok.

Intervjuperson: Jag tror att det tas förgivet att anställda inte skriver någonting negativt om företaget. Vi har dokumenterat att anställda ska tala väl om företaget, att vi inte ska säga något negativt öppet. Så det inte blir dålig publicitet för arbetet, men det står inget om just sociala medier.

Intervjuare: Ok, det du precis sa var det dokumenterat eller inte?

Intervjuperson: Jo, det är dokumenterat.

Intervjuare: Ok, Sociala medier är liksom en aspekt i vår uppsats. Den andra är då bring your own device. Tar ni med er egen utrustning till arbetsplatsen?

Intervjuperson: Det händer att kollegor samt jag själv gör det.

Intervjuare: Finns det regler för det?

Intervjuperson: Nej.

Intervjuare: Ok.

Intervjuperson: Eller vad tänker ni på för grejer?

Intervjuare: Exempelvis vad ni får ladda ner eller vilka hemsidor ni får besöka?

Intervjuperson: Inget dokumenterat.

Intervjuare: Har ni restriktioner när ni surfar på nätet?

Intervjuperson: Nej, det tror jag inte. Det är inte ok att porrsurfa liksom. Alltså jag vet inte riktigt vad som är nerskrivet, ska jag hämta dokumentet kanske?

Intervjuare: Ja, om det går bra!

Intervjuperson: Vill ni ha något? Kaffe, te, vatten?

Intervjuare: Nej tack, allt är bra.

Intervjuperson: Ok, då ska vi se här.

Intervjuare: Är det där företagets dator?

Intervjuperson: Ja, det här är företagets dator. Där finns det restriktioner att vi inte får ta hem datorn och använda den privat. För att då ska den beskattas.

Intervjuare: Ok, och det finns dokumenterat?

Intervjuperson: Nej, men eftersom jag jobbar med redovisningen så känner jag till det.

Intervjuare: Ok.

Intervjuperson: Det är något som sker ofta på andra företag, att man kan använda sin dator privat. Här tror jag att det är lite hårdare. Samma sak med mobiltelefoner, vi har en separat telefon. Alltså en privat och en jobb mobil, på grund av dagsreglerna. Annars ska de också beskattas, det är enklare med två istället.

Intervjuare: Ok.

Intervjuperson: Ska se om jag hittar dokumentet här på datorn.

Intervjuare: Baserat på de intervjuer vi har haft hittills har vi kommit fram till att de små företagen inte har någon komplett dokumenterad Internetpolicy medan de större företagen har det. Då frågor vi oss liksom när ska företag börja dokumentera regler? När har företag fått tillräckligt många anställda för att ha en sådan policy?

Intervjuperson: Två? Om du frågar mig.

Intervjuare: Så du tycker att ni borde ha en?

Intervjuperson: Jag tycker man borde ha en. Därför desto mer man har nerskrivet desto mindre risk är det att något händer.

Intervjuare: Sker det någon kontroll av era dator- och Internetanvändning? Alltså kontrollerar någon vad anställda göra på Internet här?

Intervjuperson: Inte vad jag vet.

Intervjuare: Då blir det ganska svårt och fortsätta här. Vilken position har du i företaget?

Intervjuperson: Administratör, datoransvarig.

Intervjuare: Ok, oroar du dig att anställd ska göra bort sig på nätet? Både på arbetsplatsen och privat? Exempelvis att man skriver någon olämpligt om företaget eller kanske att man uttrycker sig extremt politiskt ute på nätet?

Intervjuperson: En gång till. Om jag oroar mig för att?

Intervjuare: Att någon anställd ska göra bort sig på nätet?

Intervjuperson: Gällande företaget?

Intervjuare: Eller privat. Ja precis, både på arbetsplatsen och privat. Vi har nämligen i vår uppsats att när man kommer hem så kanske man uttrycker sig helt annorlunda på ett sätt man kanske inte göra när man jobbar. Detta beror på att man är privatperson när man kommer hem och anställd på arbetsplatsen. Som anställd har man en lojalitetsplikt och hur långt gäller den? Oroar ni er över det? Tänker ni, hoppas att han eller hon inte skriver något dumt om företaget?

Intervjuperson: Ja, nu känner jag att det inte är jag som borde svara på dessa frågor utan ledningen.

Intervjuare: Ja, det var därför vi fråga precis vilket roll i företaget du hade.

Intervjuperson: Ja, det är skillnad på mig och ledningen. Jag oroar mig inte mycket för det är inte mitt företag.

Intervjuare: Nej.

Intervjuperson: Vad folk gör privat oroar jag mig inte alls om. Jag tror inte att det är någon risk. De flesta av mina kollegor som jag haft och har skulle inte slänga ut någonting negativt på sociala medier. Det är en personlighets fråga samt en generationsfråga.

Intervjuare: Nästa fråga är ungefär besvarad. Hur känner ni om era anställdas surfvanor på fritiden? Om det är någonting som bekymrar er? Ni har inte några regler om hur anställda ska uppföra sig på nätet eller utanför arbetsplatsen.

Intervjuperson: Nej.

Intervjuare: Men händer det att medarbetarna direkt eller indirekt representerar arbetsgivaren eller företaget?

Intervjuperson: Ja, det gör man som konsult. När man är ute hos kunderna representerar man företaget och vissa kunder har i stort sett bara kontakt med en enskild konsult och känner inte resten av företaget.

Intervjuare: Ja, ok.

Intervjuperson: Men det är bara gemtemot kunder och inte på något annat sätt. Representationen mot andra nätverk och liknande står ledningen helt för.

Intervjuare: Är ni aktiva på sociala medier?

Intervjuperson: Ja.

Intervjuare: Vi skriver mycket om vilka fördelar man får om att vara aktiv.

Intervjuperson: Ja.

Intervjuare: Då ska vi se vår fina bild här. Om det är färre än tio anställda är det 28 % av alla svenska företag som har en närvaro i sociala medier från 2013. Har företagen minst 250 anställda är det 69 %.

Intervjuperson: Ok.

Intervjuare: Detta kanske inte är en prioritet för er? Just nu.

Intervjuperson: Nej, det är det inte.

Intervjuare: Ja, sant. Det här med att ni tar med er tekniska utrustning, vad anser du är fördelarna med det?

Intervjuperson: Att man kan använda det man behöver. Jag vet att folk har tagit med tangentbord för att det är jobbigt med bärbar och när man har en skärm så blir det ännu lättare med ett tangentbord. Folk har även tagit med stolar och skärmar för att de inte har varit bekväma med de som redan finns. Brist på utrustning helt enkelt så tar man med hemifrån för att lösa sina akuta problem.

Intervjuare: Har ni ett eget nätverk?

Intervjuperson: Ja.

Intervjuare: Får ni koppla upp er till det nätverket med er egen utrustning? Exempelvis er egen mobil eller bärbara dator?

Intervjuperson: Ja.

Intervjuare: Finns det några problem med det här? Har det skett någon incident?

Intervjuperson: Nej, inte vad jag vet.

Intervjuare: Ni tar helt enkelt med det för att ni är bekväma med er egen utrustning?

Intervjuperson: Ja, en av mina kollegor använder sin egen mobil för både arbete och privat för att jobb mobilen inte funkar riktigt. Hon betalar det själv, men det är inga stora summor.

Intervjuare: Ja, ok. Detta gick ganska snabbt men sista frågan kommer här. Har det hänt någonting tidigare? Alltså finns det exempel på en tidigare händelse där era anställdas dator-

och Internetanvändning på något sätt har skapat problem för företaget? Någon konflikt eller situation?

Intervjuperson: Nej, inte riktigt.

Intervjuare: Nej? Allt har varit perfekt?

Intervjuperson: Ja, eller specificera det igen?

Intervjuare: Ja, någon tidigare händelse där något har gått fel med någon anställd. Exempelvis andra företag har sagt att deras anställd har besökt någon sida som de inte fick besöka och det har uppstått lite problem. Eller någon kanske tog med sig egen dator till arbetsplatsen och koppla upp sig med företagets nätverk och de var massa pornografika filmer på datorn. Lite drastiskt och stort men något sådant eller något litet som har hänt.

Intervjuperson: Jag har inte hört talas om någon har surfat på någon sida som inte har varit ok.

Intervjuare: Men det vet du samtidigt inte?

Intervjuperson: Nej, jag vet inte men jag har inte hört någonting om det heller.

Intervjuare: Ni kontrollerar inte det heller?

Intervjuperson: Nej. Jag kontrollerar inte det, men kanske ledningen gör?

Intervjuare: Händer det att anställda kanske tar med sin dator någon gång bara sådär och vill uppdatera den eller kanske säger att de ska uppdatera den?

Intervjuperson: Det är jag som uppdaterar företagets datorer.

Intervjuare: Jaha ok.

Intervjuperson: Men vi låser in alla datorer på kvällen efter arbetspasset. När jag inte är här så vet jag inte vad de gör med datorerna, de kanske kontrollerar dem då. Vi har inloggningslösenord och de har de tillgång till, samt mailen. Det kan vara ett sätt som de kontrollerar datorerna, det har jag inte en minsta aning om.

Intervjuare: Ja, ok.

Intervjuperson: Ni kanske borde prata med VD:n om dessa frågor han vet förmodligen mer om det.

Intervjuare: Ja, det har varit bra. Går det och få hit honom?

Intervjuperson: Ja, jag ska kolla om han kan.

Intervjuare: Han är här?

Intervjuperson: Ja.

Intervjuare: Det hade varit riktigt bra om vi hade kunnat få in honom i intervjun.

Intervjuperson: Ja, jag tror det hade hjälpt er mer.

Intervjuare: Vi tänkte på en annan grej, pratar ni om det överhuvudtaget? Om detta ämne?

Intervjuperson: Vår chef har sagt någon gång att de inte vill att de anställda spelar spel på sin utrustning på arbetstid. Det är det enda jag tror de har nämnt. Mer än det har vi inte pratat om.

Intervjuare: Ok. Det känns som att det inte är något ni bekymrar er med, eftersom ni då är ett mindre företag kan vi tänka oss?

Intervjuperson: Ja.

Intervjuare: Det känns också som att ni alla litar på varandra?

Intervjuperson: Ja, man märker snabbt om någon inte jobbar. Jag tror även att de som jobbar här vet att det är svårt att göra sitt arbete om man vill maska. Man märker hur mycket arbete varje anställd gör på deras arbetstider. Det är ganska mycket uppföljning på vad medarbetarna gör med sin tid.

Intervjuare: Vi skriver det i vår uppsats. Som det här med sociala medier, först så tänker man att de anställda sitter på sidor och inte får mycket gjort. Men sen har dessa utvecklats till en plats där man kan skriva något som kan liksom få hela företaget att kollapsa om man skriver eller publicerar något riktigt dumt.

Intervjuperson: Ja.

Intervjuare: Vår fråga då om vi går bort lite från det här. Har du arbetat på ett tidigare företag där du känner att du kanske kan svara mer? Exempelvis sista frågan, som var om någon incident har hänt?

Intervjuperson: Jag har haft kollegor som inte var villiga att arbeta. Som inte vill arbeta, ägna större delen av dagen att maska.

Intervjuare: Det var då att surfa runt på sociala medier?

Intervjuperson: Nej, detta var så länge sen. Det var förre smartphones tider.

Intervjuare: Ok.

Intervjuperson: Ja, det var inte datoranvändning då på 90-talet. Jag arbetade natt inom vården och hade en kollega som sov sig igenom natten och arbetade så lite som möjligt. Det är liksom en annan sorts människor som har den inställningen, att de ska arbeta så lite det bara går.

Intervjuare: Oj, ok.

Intervjuperson: Ja, och den typen av kollegor har jag inte haft här. Det tror jag är en personlighetsfråga, men jag tror att det bara sker på större företag.

Intervjuare: Ja.

Intervjuperson: På min förra arbetsplats tror jag Internetanvändningen var mycket större. Jag tror även att det fanns en acceptans på företagets anställas användingen av sociala medier. Tar man en fem minuters paus då och då så är det väl ok.

Intervjuare: Ja. Där fanns allting dokumenterat? Eller någon Internetpolicy?

Intervjuperson: Jag jobbade som konsult där men jag tror att de hade, jag tror framförallt att de har en policy idag.

Intervjuare: Om företaget har en Internetpolicy så måste alla anställda få reda på det. Då frågar vi liksom hur de får reda på det, det är en fråga här. Men i och med att ni inte hade en Internetpolicy så fråga vi aldrig dig det.

Intervjuperson: Ja, nej men jag hittar inget specifikt i vår dokumentation just nu.

Intervjuare: Jag tror inte vi har mycket mer och fråga om faktiskt. Kunde vi intervju VD:n lite snabbt?

Intervjuperson: Ja, jag tror ni ska ställa de lite känsligare frågorna till honom faktiskt. När det gäller dator- och Internetanvändning. Ska kolla om han kan komma in.

Intervjuare: Ja, tack.

Intervjuperson 2: Hallå grabbar!

Intervjuare: Hej!

Intervjuperson 2: Jag har lite bråttom idag så jag skickade in henne lite snabbt. Jag kan ta över de som hon tyckte var lite jobbigt att svara på. Jag ska iväg snart men vi kan ta ett par minuter. Frågan hon ställde mig precis var om vi kontrollerar våra anställdas Internetanvändning, och det gör vi inte. Det borde hon veta men hon är så ödmjuk.

Intervjuare: Ok, ingen fara. Då är vår följd fråga, finns det någon anledning till varför ni väljer och inte övervaka?

Intervjuperson 2: Vi anser att det inte finns någon anledning åt att göra det.

Intervjuare: Ja, finns det någon anledning till varför ni avstår att övervaka?

Intervjuperson 2: Vi kan mäta våra anställdas resultat. De ska debitera sitt arbete på respektive kund, och vi har ett debiteringskrav. ”Av din arbetstid ska du debitera så här mycket procent”, gör de det så bra. Om de debiterar tre timmar på en kund och de bara surfat på Internet så kommer kunden reagera. Så vi har ingen anledning för att övervaka anställdas, det är inte den sortens arbete som gör att anställda kan sitta och surfa eller göra en massa saker ute på Internet. Tar man sedan fem minuter och kollar sin facebook eller kollar något annat så är det ok, man kan ta några minuter paus varje timme.

Intervjuare: Vi sa till henne när anställda tänker på sociala medier på arbetsplatsen. Då tar det oftast några minuter att gå in på hemsidan och göra vad de vill, sen helt plötsligt har det gått

en timme. De hemsidorna har blivit att man skriver saker som kan vara helt oacceptabelt för företagets ledning, som kan skada företaget. Då frågar vi liksom om du oroar dig för att anställda ska skriva något olämpligt på hemsidor under arbetstid samt privat?

Intervjuperson 2: Nej, det gör jag inte. Egentligen handlar det mycket om att rekrytera rätt tänker jag. Om någon vill skada företaget kan man aldrig riktigt 100 procent skydda.

Intervjuare: Nej, det måste inte vara skada. Det kan vara så att de uttrycker sig exempelvis extremt politiskt.

Intervjuperson 2: Ja, men det är samma sak. Det har företag alltid kunnat drabbas av, det är bara synligt på ett annat sätt nu tack vare Internet. Det finns inte resurser och tid för att lägga upp system inom företaget för att kolla detta, när vi har ett litet företag.

Intervjuare: Ja, det är sant.

Intervjuperson 2: Det finns inte direkt några affärshemligheter, som alla uppfinnar företagen har. Där är det mycket känsligare, för om du sticker som anställd och tar med dig en algoritm i huvudet till en konkurrent så är det mycket värre. Men vårt arbete är liksom inte så känsligt. Ja, det är klart att om någon vill göra djävelskap på det här företaget skulle kunna basunera ut att det här företaget gör så här eller något. På detta sätt skulle de kunna skada oss. Då är det en människa som har blivit bitter, och det finns en konflikt. Detta kan man inte bädda för i förväg utan det får man ta då. Det vi gör är inte några hemligheter precis, det finns inte några patentfrågor eller industri spinoffs.

Intervjuare: Ja, vi sa det också till henne att vi har intervjuat ett par företag. De företagen som har varit små har inte haft en Internetpolicy och de stora har haft en Internetpolicy. Frågan är då när ska företag skaffa sig en Internetpolicy?

Intervjuperson 2: Ja, det är intressant. Vilket jag inte kan svara på, utan det är något ni ska forska fram.

Intervjuare: Ja, precis. Men om vi säger att du har 50 anställda skulle du tänka dig ha en Internetpolicy?

Intervjuperson 2: Jag kan inte riktigt se mig ha 50 anställda men ja, det skulle jag nog kunna ha. Sedan är det inte så simpelt med att bara ha en Internetpolicy utan man måste ha något system för att följa upp policyn.

Intervjuare: Ja, det är då kontroll exempelvis.

Intervjuperson 2: Ja, det kan vara kontroller, möten, seminarium eller bjuda in experter. Viktigare än kontroll tänker jag skulle varit att man har ett seminarium om exempelvis ”Vad händer om du gör så här?”, ”Var finns dina spår på Internet?”. Den kunskapen, hur många har det i Sveriges befolkning? Att de sitter och delar samt surfar, vad händer? Det tror jag är väldigt få som förstår. Det skulle vara det som skulle varit intressant och hade kunnat göra något med. Vi är väldigt fokuserade på att lägga upp policy för vårt arbete, vilket är svårt nog. Att alla ska arbeta lika mycket, alla ska bokföra lika och alla kunder ska jobba efter ett visst

system. Efter alla år är detta något vi fortfarande inte är framme vid vårt mål, vilket är något vi fokuserar på.

Intervjuare: Ja, ni prioriterar inte detta förstås.

Intervjuperson 2: Nej precis, vi får ha ett slags förtroende för våra anställda.

Intervjuare: Precis, ni litar på varandra. Är det ok för er att anställa tar med exempelvis egen utrustning och kopplar upp sig till ert företags nät?

Intervjuperson 2: Ja, de har ingen egen utrustning med sig. Alla har en egen företags dator och mobil.

Intervjuare: Händer det att dem tar med sig egen dator?

Intervjuperson 2: Nej, det har aldrig hänt. Aldrig varit något problem.

Intervjuare: Så de tar inte med sig en egen dator, laptop eller surfplatta?

Intervjuperson 2: Nej, absolut inte. Det har inte hänt.

Intervjuare: Det får de göra eller?

Intervjuperson 2: Det har inte hänt, så jag vet inte. Skulle man hellre sitta här på lunchen istället för att äta, om man nu hade någon speciellt anledning för att sitta på sin egen utrustning och håll på så är det helt ok. Men detta har aldrig hänt så jag vet inte.

Intervjuare: Ok, vi vet inte hur lång tid du har på dig men ska vi fortsätta?

Intervjuperson 2: Ja, jag har en kund jag måste gå till. Fem minuter till bara, sen måste jag gå.

Intervjuare: Två snabba frågor till.

Intervjuperson 2: Ja, självklart.

Intervjuare: Ok, anställda på fritiden, vad de gör på nätet, sociala medier, allt sånt är det något du oroar dig för?

Intervjuperson 2: Nej, inte riktigt. Jag tänker inte på det.

Intervjuare: Har det hänt någon gång en tidigare händelse eller situation där dator- eller Internetanvändning har skapat någon sorts incident? Exempelvis någon dålig hemsida eller liknande.

Intervjuperson 2: Nej, inget som har kommit fram på bordet.

Intervjuare: Pratar ni om det? Alltså pratar ni om det med varandra? Vad får vi göra, vad får vi inte göra?

Intervjuperson 2: Nej, faktiskt inte. Men jag tror att det står i vårt anställningskontrakt, jag kommer inte ihåg formuleringen men en allmän formulering finns med naturligtvis. Det kan

vara mobiltelefon, innan Internet fanns arbetade jag på arbetsplatser där det blev lite problem om man pratade privat telefon. Det är klart det spåras inte över hela världen men det stör arbetet lika mycket som att man lägger ner massa tid på det man inte ska göra. Men återigen jag tycker vi har det lättare mätbart här, jag har andra kunder som där det inte ens går att mäta. Där ska du som anställd leverera någon slags luddigare sak, du sitter på ett IT företag och ska leverera. Det är lite svårare och mäta, det blir att man ska levererar något och man får det inte klart samma dag som planerat utan det blir senare. Det är lite svårare och mäta upp det, här har vi det ganska mer konkret.

Intervjuare: Ni märker det tydligare.

Intervjuperson 2: Tidsmässigt märker vi det, de andra frågorna som exempelvis kan det skada oss och liknande. De frågorna är det lite svårare, för de märker vi inte. Där är det återigen en slags förtroende fråga.

Intervjuare: Brukar du ta hem arbete?

Intervjuperson 2: Det händer att någon kan göra det, ja. Det är mest en person som brukar göra det, de flesta brukar stanna här och jobba övertid.

Intervjuare: Då tänkte vi mer som exempelvis om de då tar hem arbetsdatorn och arbetar med den och kan då sitta och göra vad som helst hemma privat.

Intervjuperson 2: Ja, självklart. Men det kan man göra här också egentligen. Jag kan sitta här tio timmar men jag debatterar bara åtta timmar, då märks det inte om jag sitter kvar två timmar och göra privata saker på min arbetsdator.

Intervjuare: Ja, det var nog allt! Tack ska du ha för din tid. Det var bra faktiskt.

Intervjuperson 2: Var det bra?

Intervjuare: Ja, nu kan vi analysera mera. Har vi gjort så att du har fått lite tankar nu eller?

Intervjuperson 2: Ja, det har det. Det är bra att få lite inputs faktiskt. Det kanske inte har hänt någonting om något år, men det vet vi aldrig. Men det är jätte bra att man får en tankeställare, självklart.

Intervjuare: Kanske kolla igenom arbetsdatorerna när ni göra uppdateringar i framtiden?

Intervjuperson 2: Ja, det kan vi faktiskt göra. Jag fick faktiskt göra lite något på min förra arbetsplats för att ingen annan kunde och jag var lite kunnig i det området. Så om vi växer kanske vi börjar tänka på detta och implementera något eller anliter någon som löser det åt oss.

Intervjuare: Det låter som att du är väldigt erfaren inom detta. Det kanske finns någon annan incident du kanske kommer på om vi återgår till den sista frågan igen?

Intervjuperson 2: Nej, det var nog bara den lilla incidenten.

Intervjuare: Ja ok, tack så mycket återigen.

Intervjuperson 2: Tack själva. Lycka till! Är det en kandidatuppsats detta eller?

Intervjuare: Ja, precis.

Intervjuperson 2: Hade varit trevligt om jag hade kunnat få se hur den slutar då.

Intervjuare: Ja, absolut. Vi kan skicka en kopia senare om du vill.

Intervjuperson 2: Ja, nu måste jag springa iväg. Tack och hej. Lycka till!

Intervjuare: Tack själv! Hej då!

B5 – Mail till respondenterna

Hej!

Vi är två studenter från Ekonomihögskolan i Lund som studerar Systemvetenskap. Vi skriver för närvarande vår kandidatuppsats om den syn som finns i företag om anställdas dator- och Internetanvändning. Detta innebär att vi behöver genomföra en empirisk undersökning och skulle gärna vilja intervjua en representant från ert företag.

Vi skulle uppskatta om vi kunde besöka er verksamhet och prata med er på plats, om ni vill hjälpa oss att genomföra vårt projekt. Om ni hellre skulle vilja genomföra en intervju via telefon, så går detta också bra. Skriv gärna då vilka tider som passar er. Vi hoppas att ni vill medverka i vår undersökning.

Tack på förhand,

Jan och Ashkan

Referenser

BBC (2012): BYOD: Bring your own device could spell end for work PC
Tillgänglig: http://www.bbc.co.uk/news/business-17017570
(2014-05-01)

Bilan, C. & Hedberg, C. (2001): Säkerhetshot och lösningar för privatpersoner med bredband
Tillgänglig:
http://www.bth.se/fou/cuppsats.nsf/all/ae1ab3343c618ca8c1256a65002f46be/$file/s%C3%A4kerhetshot%20och%20l%C3%B6sningar%20f%C3%B6r%20privatpersoner%20med%20bredband.doc
(2014-05-15)

BusinessZone (2013): The Advantages and Disadvantages of BYOD
Tillgänglig: http://www.businesszone.co.uk/blogs/scott-drayton/optimus-sourcing/advantages-and-disadvantages-byod
(2014-05-05)

Bylund, M. (2013): Personlig integritet på nätet
Tillgänglig: http://personligintegritet.se/wp-content/uploads/2013/11/FORES-Personligintegritet_web_enkelsid.pdf
(2014-05-01)

CIO Sweden (2012): Analytiker sågar BYOD
Tillgänglig: http://cio.idg.se/2.1782/1.476879/analytiker-sagar-byod
(2014-05-15)

CIO Sweden (2013): Så växer BYOD 2013
Tillgänglig: http://cio.idg.se/2.1782/1.500075/sa-vaxer-byod-2013
(2014-05-15)

Cisco (2013): New Analysis: Comprehensive BYOD Implementation Increases Productivity, Decreases Costs
Tillgänglig: http://blogs.cisco.com/news/new-analysis-comprehensive-byod-implementation-increases-productivity-decreases-costs/
(2014-05-15)

Datainspektionen (2003): Behandling av personuppgifter för kontroll av anställda, Datainspektionens rapport 2003:3
Tillgänglig: http://www.datainspektionen.se/Documents/rapport-personuppgifter-anstallda.pdf
(2014-05-01)

Datainspektionen (2005): Övervakning i arbetslivet, Kontroll av de anställdas Internet- och e-postanvändning m.m. Datainspektionens rapport 2005:3
Tillgänglig: http://www.datainspektionen.se/Documents/rapport-overvakning-arbetslivet.pdf
(2014-05-01)

Datainspektionen (2013): Användning av anställdas egen utrustning i tjänsten, så kallade Bring Your Own Device-lösningar, BYOD
Tillgänglig: http://www.datainspektionen.se/personuppgiftsombud/samradsyttranden/mall2/
(2014-05-01)

Delphi (2013): Övervakning i arbetslivet, vad är egentligen tillåtet?
Tillgänglig: http://www.delphi.se/$-1/file/artiklar/2013/131129-skydd-och-sakerhet-nr-8-2013-daniel-lundqvistfredrik-gustafsson.pdf
(2014-05-05)

Dimensional Research (2012): The impact of mobile devices on information security: A survey of IT professionals
Tillgänglig: http://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf
(2014-05-01)

Findahl, O. (2011): Svenskarna och Internet 2011
Tillgänglig: https://www.iis.se/docs/SOI2011.pdf
(2014-04-11)

Findahl, O. (2013): Svenskarna och Internet 2013
Tillgänglig: https://www.iis.se/docs/SOI2013.pdf
(2014-04-20)

Gartner (2012): Gartner Identifies Three Security Hurdles to Overcome When Shifting From Enterprise-Owned Devices to BYOD
Tillgänglig: http://www.gartner.com/newsroom/id/2263115
(2014-05-05)

IT & Telekomföretagen (2013): Ta fram en e-post- och Internetpolicy
Tillgänglig: http://www.itotelekomforetagen.se/arbetsgivarguiden/datoranvandning/ta-fram-internetpolicy?expanded_accordions=acc_1,acc_1_1,acc_1_2&tabascoSelected=tb_1
(2014-05-05)

Jacobsen, D.I. (2002): Vad, hur och varför? Om metodval i företagsekonomi och andra Samhällsvetenskapliga ämnen.

Junesjö, K. (2000): Distansarbete, datorer, integritet. Handbok för anställda
Tillgänglig: http://www.kurt.nu/bocker_text/Distansarbete.pdf
(2014-04-28)

Justitiedepartementet (1991): Yttrandefrihetsgrundlag (1991:1469)
Tillgänglig: http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Yttrandefrihetsgrundlag-1991_sfs-1991-1469/?bet=1991%3A1469
(2014-05-01)

Justitiedepartementet (1998): Personuppgiftslag (1998:204)
Tillgänglig: http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Personuppgiftslag-1998204_sfs-1998-204/?bet=1998:204
(2014-05-01)

LunaMetrics (2011): 6 Benefits of social media for business
Tillgänglig: http://www.lunametrics.com/blog/2011/06/08/6-social-media-benefits-for-business/#sr=g&m=o&cp=or&ct=-tmc&st=(opu%20qspwjefe)&ts=1400770095
(2014-05-04)

Simmers, C.A. & Bosnian, M. (2002): Reducing legal, financial, and operational risks: A comparative discussion of aligning Internet usage with business priorities through Internet Policy Management.

Statistiska Centralbyrån (2013): Företagens användning av IT 2013
Tillgänglig:
http://www.scb.se/Statistik/_Publikationer/NV0116_2013A01_BR_IT02BR1401.pdf
(2014-05-03)

Stepstone (2013): Rekrytering via sociala medier – bra eller bara hype?
Tillgänglig: http://www.elwirakotowska.se/wp-content/uploads/2011/11/Rekrytering-via-sociala-medier-2013-bra-eller-bara-hype.pdf
(2014-05-03)

Teknikföretagen (2013): Lojalitetsplikten och Internet.
Tillgänglig:
http://www.teknikforetagen.se/Documents/Arbetsratt/Lojalitetsplikten_och_internet.pdf
(2014-05-04)

Transportgruppen (2012): Anställda och sociala medier
Tillgänglig:
http://www.transportgruppen.se/Documents/Publik_F%C3%B6rbunden/BA/Om%20BA/BA%20skriver%20i%20Akeritidningen/Artikel%207-8%20Sociala%20medier.pdf
(2014-05-03)

VMware (2013): The BYOD Opportunity, Say "Yes" to Device Diversity and Enable New Ways to Drive Productivity
Tillgänglig: http://www.vmware.com/files/pdf/view/VMware-BYOD-Opportunity-Whitepaper.pdf
(2014-05-05)

Welebir, B. & Kleiner, B. (2005): How to write a proper Internet usage policy. Management Research News, 28(2), 80-87.
Tillgänglig: http://www.aslib.co.uk/journals.htm?issn=0140-9174&volume=28&issue=2&articleid=1501895&show=pdf
(2014-04-11)

Åbo Akademi (2012): Informationssäkerhet och sociala medier
Tillgänglig: http://web.abo.fi/dc/admin/reglerlagar/Sociala_medier_informationssakerhet.pdf
(2014-05-15)