GÖTEBORGS UNIVERSITET

Den levande policyn

Säkerhetsaspekter kring mobila Business Intelligence-lösningar och Bring Your Own Device

The living policy

Security aspects in mobile Business Intelligence solutions and Bring Your Own Device

JACOB LANDÉN
ANTON SUNDH

Kandidatuppsats i Informatik

Rapport nr. 2013:037
ISSN: 1651-4769

Göteborgs universitet
Institutionen för tillämpad informationsteknologi
Göteborg, Sverige, Maj 2013

Abstrakt

Fler och fler företag inser nyttan med att analysera företagsinformation och på sätt hålla sig konkurrenskraftiga i dagens föränderliga samhälle. Genom att använda sig av beslutsstödsystem, så kallat Business Intelligence (BI) kan organisationer samla ihop och bearbeta företagsdata och på så sätt få ut mer av sin verksamhet.

Idag räcker det inte längre för organisationer att ha tillgång till företagsinformation innanför kontorets väggar, man måste även kunna ha med sig informationen "on the go", vilket har legat till grund för framfarten och utvecklingen av *mobila BI-lösningar*. I och med att mobiliteten ökar och att företagsdata lämnar kontoret så uppkommer nya risker, vilket är en anledning till att många företag tvekar vid tanken på att införa mobila BI-lösningar.

Vi har i denna uppsats undersökt två säkerhetsaspekter inom området kring mobila BI-lösningar, och utformat vår frågeställning enligt följande: *Hur spelar säkerhetsaspekter in i ett företags beslut att anskaffa mobila BI-lösningar?* Undersökningen har genomförts genom intervjuer i samarbete med företaget Optivasys som uteslutande arbetar med BI-lösningen QlikView.

Mycket av den teori vi studerat beskriver säkerhetsaspekter som kritiska, däremot har vi under undersökningen sett en lösning på hur företag kan hantera säkerhetsaspekter. Denna lösning är i form av en levande policy, dvs. en policy som uppdateras med åren och som på så sätt kan hantera nya risker.

Nyckelord: Business Intelligence, mobilitet, mobil Business Intelligence, BYOD, policy, QlikView, säkerhet.

Abstract

In today's changing environment, an increasing number of companies are realizing the benefits of analyzing business information and thereby stay competitive. By making use of decision support systems, known as Business Intelligence (BI), organizations are expected to collect and process business data and thus get more out of their business.

Nowadays it is not enough for organizations to have access to corporate data inside office walls, they must also be able to bring the information "on the go", which has been the foundation for the progress of mobile BI solutions. As the mobility increases and the corporate data leaves the office, new risks arise, which is one reason as to why many companies hesitate at the idea of introducing mobile BI solutions.

In this paper we explore two security aspects in the area of mobile BI solutions. Our research question is as follows: *How does security aspects affect a company's decision to acquire mobile BI solutions?* The survey was conducted through interviews in cooperation with the firm Optivasys, exclusively dedicated to the BI solution QlikView.

A significant part of the theory we studied describes security as critical; however, our research suggests a solution on how companies can manage the security aspects. This solution is in the form of a living policy, i.e. a policy that is updated through the years and therefore can deal with new risks.

Keywords: Business Intelligence, mobility, mobile Business Intelligence, BYOD, policy, QlikView, security.

TACK

Vi vill tacka Optivasys, och då främst Helena Wallström och Oskar Gröndahl för möjligheten att genomföra denna undersökning. Tack för hjälpen med kontakt till informanter och tack för feedback under arbetets gång.

Tack till de informanter som har ställt upp och gett oss värdefull input till undersökningen. Tack för att ni tog er tid att hjälpa oss.

Vi vill även tacka vår handledare Lisen Selander för allt stöd och den feedback vi fått.

Innehåll

1. Introduktion

Business Intelligence (BI) blir ett allt viktigare verktyg för företag vid beslutsfattande. BI fungerar som en hjälp i att samla och behandla företagsdata, genom att förena sådan data som en gång varit utspridd och fragmenterad (Kuntze et al, 2010). BI har länge varit någonting som enbart större företag har kunnat använda och endast ett fåtal tekniskt kunniga personer inom företagen har förstått (Lawton, 2006; Talati et al, 2012). Detta har lett till att det har gått långsamt att hantera och analysera data, vilket i sin tur har lett till att BI inte har kunnat användas i dagligt beslutsfattande (Lawton, 2006). Från att BI endast har kunnat användas av ett fåtal personer inom ett företag går utvecklingen nu mot att man vill utveckla BI-applikationer som kan användas av en större del av organisationen (ibid).

Kortfattat kan BI beskrivas som olika datoriserade processer som förbättrar beslutsfattande i organisationer, genom att transformera data till information och slutligen till kunskap (Popovic et al, 2012). Definitionerna av BI varierar en aning (se t.ex. Talati et al, 2012), men i fortsättningen kommer vi referera till ovanstående definition.

Den ökade tillgängligheten och prestandan i mobila enheter har gjort det möjligt för företag att även använda BI mobilt (Kuntze et al, 2010). Detta har gjort att användning av företagsdata i mobilen har kommit att bli en självklarhet för företag. De mobila lösningarna gör det möjligt för företags anställda att inte vara låsta vid sitt skrivbord då de vill ha omedelbar tillgång till data exempelvis då de är ute hos kunder. Möjligheten till att fatta snabba beslut kan genom användning av mobilt BI öka konkurrenskraften hos företag, exempelvis med hjälp av dess förmåga att generera realtids-data (Airinei & Homocianu, 2010). Trots alla fördelar med mobila enheter finns det ett flertal risker som användning av dessa enheter medför (Kuntze et al, 2010; Rose, 2013). Rose (2013) skriver om tre kategorier av risker; fysiska, interna och användarrelaterade. Den fysiska kategorin innefattar risker med att enheterna lämnar organisationen och att de lätt kan tappas bort eller bli stulna, medan den interna kategorin handlar mer om datasäkerhet. Den användarrelaterade kategorin tar upp organisatoriska policies om användning och hantering av enheterna.

Enligt en undersökning gjord av Computerworld år 2012, menar hälften av de tillfrågade IT-cheferna att de utarbetat strategier för riskhantering av mobila enheter inom företaget. I samma undersökning svarar de även på frågan om en formell hanteringsstrategi för dessa mobila enheter har arbetats fram och endast 46 % säger att en sådan strategi har införts (Violino, 2012).

1.2 Problem

Idag finns mycket forskning kring säkerhet i mobila enheter, men forskningen behandlar främst datasäkerhet och dataöverföring (se t.ex. Kuntze et al, 2010; Rose, 2013; Oberheide et al, 2008). Relativt lite forskning har beskrivit andra säkerhetsaspekter så som företags policies och användning av mobila enheter, däremot visar denna forskning på att en ökad medvetenhet börjar utvecklas inom detta område (se t.ex. Rose, 2013; Violino, 2012; Chaudhry, 2012).

Enligt Libiszewski (se Violino, 2012 s. 32) kommer ett stort fokus i framtiden ligga på att anställda har med sig sina egna enheter till arbetet, ett område som benämns "Bring Your Own Device" (BYOD).

"I anticipate BYOD being an area of focus in 2013, and therefore I may seek help with anything from writing the policy to evaluating and implementing solutions for mobile device firewalls, [antivirus tools] and management software" (Libiszewski, se Violino, 2012 s. 32).

Riskerna med att företag blir mer mobila ökar i och med att anställda tar med sig sina egna enheter, detta gör det svårare för företagen att ha kontroll på sin företagsdata (Violino, 2012; Chaudhry, 2012).

"The biggest threat that enterprises face is the loss or theft of devices containing enterprise data" (Jain, se Violino, 2012 s. 32).

I och med detta kan det vara viktigt för företag att upprätta policies som beskriver hur anställda får hantera företagsinformation på mobila enheter. Ju längre ett företag väntar med att införa en policy för användandet av företagsdata på egna enheter desto känsligare blir man för dataläckage och andra risker (Chaudhry, 2012).

1.3 Syfte och frågeställning

Vårt syfte med uppsatsen är att undersöka specifika risker med mobila Business Intelligence tjänster och om dessa risker spelar in när företag ämnar anskaffa mobilt BI.

Utifrån vårt syfte har vi utformat följande frågeställning:

Hur spelar säkerhetsaspekter in i ett företags beslut att anskaffa mobila BI-lösningar?

För att besvara vårt syfte och frågeställning kommer vi främst att utgå från två huvudsakliga teman:

- Företags inställning till policies kring användande av mobilt Business Intelligence/BYOD och de säkerhetsrisker som detta medför.
- Säkerhetsaspekter kring den mänskliga faktorn (borttappade/stulna enheter).

1.4 Definition och avgränsning

En viktig avgränsning i vår frågeställning handlar om definitionen av de säkerhetsaspekter som vi kommer undersöka. Definitionen av säkerhetsaspekter är i den här studien relaterad till de teman som vi presenterat ovan. Den största delen av tidigare forskning handlar, som vi tidigare nämnt, om datasäkerhet, vilket vi inte kommer behandla i denna uppsats.

Undersökningen kretsar kring BI-verktyget QlikView som vi kommer gå in närmare på i avsnitt 4.1.

1.5 Undersökningens upplägg

I kapitel 2 kommer vi att redovisa teoristudier som är relevanta för undersökningen. Kapitlet förväntas ge insikter om BI generellt och mobila lösningar av BI i synnerhet. Detta för att läsaren ska få en bättre förståelse för den vidare undersökningen och det system vi kommer bygga vår fallstudie runt.

Det teoretiska ramverk vi kommer att använda oss av går vi igenom i kapitel 3. Här diskuterar vi de säkerhetsaspekter som vårt arbete kommer att behandla, närmare bestämt *mänskliga faktorer* och *policies/BYOD*. Genom att förklara vad dessa aspekter betyder och hur man förhåller sig till dem i dagsläget hoppas vi kunna förmedla en bra bild över synen på dessa säkerhetsaspekter.

I studien kommer intervjuer genomföras med företag som använder en specifik mobil BI-lösning där målet är att skapa en förståelse för hur företag ser på de säkerhetsaspekter som vi fokuserat på i denna undersökning. Den specifika mobila BI-lösningen kommer att presenteras i kapitel 4 tillsammans med vårt tillvägagångssätt för studien, där vi presenterar de metoder och tekniker som vi har använt oss av. I kapitel 5 går vi igenom det resultat vi fick fram från intervjuerna och i kapitel 6 analyserar vi detta resultat för att sedan presentera våra slutsatser i kapitel 7.

2. Relaterad litteratur

Avsnittet kommer att behandla BI och mobila BI-lösningar, vårt fokus i avsnittet kommer ligga på att definiera dessa begrepp närmare och belysa hur de används idag. Vi kommer börja med att diskutera BI för att ge en övergripande förklaring till begreppet, sedan går vi in på området kring mobila BI-lösningar för att ge en bättre bakgrund till just vår undersökning. Genom att söka i olika artikeldatabaser har vi valt ut litteratur som är relevant för uppsatsen och de begrepp vi vill diskutera.

2.1 Business Intelligence

Business Intelligence (BI) är ett brett begrepp som vanligtvis associeras med företagsinformation, information i form av statistik eller andra råa format som visar dagliga aktiviteter i företag (Talati et al, 2012). Termen BI är ett populariserat paraplyuttryck, myntat och främjat av Howard Dresner på Gartner Group 1989. Det beskriver en samling koncept och metoder som förbättrar företags förmåga att ta beslut (Power, 2007). BI kombinerar företagsdata med analyseringsverktyg för att presentera komplex och konkurrenskraftig information för beslutsfattare. Målet med detta är att förkorta och förbättra beslutsprocesser genom att förstå vad företag är kapabla till. Detta görs genom att analysera trender och situationer på olika marknader och konceptet är, enligt Negash (2004) absolut nödvändigt för att hantera stora företag i dagens samhälle. BI kan ibland vara en synonym för Competitive Intelligence (CI), då båda fungerar som beslutsstöd. Skillnaden är dock att BI framförallt hanterar intern data och arbetsprocesser, till skillnad från CI som hanterar och analyserar data från konkurrenter till företaget (Negash, 2004).

Fördelarna med att implementera BI i sin organisation är att man kan öka kunskapen och förståelsen om sin verksamhet på många sätt. Exempelvis kan man få snabbare tillgång till information, utföra snabbare utsökningar och analyser, få en högre grad av interaktivitet med sin data och rent generellt hjälpa till med datahanteringen (Popovic et al, 2012).

Många av de traditionella BI-systemen består av flera element som inte alltid fungerar bra tillsammans, detta i kombination med olika typer av datakällor vars information inte heller fungerar bra då de integreras med varandra. Dessa svårigheter gjorde BI-systemen långsamma när det gällde att samla ihop och analysera data, vilket ledde till att teknologin inte var användbar i dagliga analyser för beslutsfattande. Dagens BI har åtgärdat dessa problem och mycket av fokus ligger nu istället på att generera realtidsdata och skapa användarvänliga gränssnitt så att fler och fler kan använda teknologin (Lawton, 2006).

2.2 Mobila BI-lösningar

Det traditionella sättet att arbeta med BI, då data bara var åtkomlig inom kontorets gränser, är över. Eftersom beslutsfattande äger rum på många platser behöver de ansvariga ha med sig sitt BI-system överallt. Dagens internetuppkopplade mobila enheter har skapat de förutsättningar som behövs för att stödja detta behov (Power, 2013; Stipic & Bronzin, 2011). Airinei och Homocianu (2010) menar att ha tillgång till företagsdata mobilt är snarare en regel än ett undantag i dagens företagssamhälle. De mobila beslutsstöden kan tillhandahålla tjänster baserade på geografisk plats och göra realtidsanalyser baserade på den kontext man befinner sig i. Det kan vara t.ex. en återförsäljare som behöver komma åt sin data snabbt och smidigt då de besöker sina olika butiker, och inte bara ha tillgång till sin data från kontoret. Faktumet att man har med sig sina mobila enheter dygnet runt kan göra så att användandet av BI-systemet ökar och därmed kunskapen om företagets data (Airinei & Homocianu, 2010).

Utmaningen för de som utvecklar mobilt BI är att förutse vilka data en användare behöver och när de behöver den. Därför består den generella strukturen i gränssnittet av flertalet tabeller, statistik, varningar, grafer av trender, diagram och till och med kartor. De som designar applikationen måste även ta hänsyn till den mindre skärmen som de mobila enheterna har vilket gör att det blir svårare för användare att se detaljerade grafer och liknande. Huvudfunktionen i dessa system är dynamiken då de stödjer OLAP-funktioner (Online Analytical Processing) så som drill-down och roll-up (Airinei & Homocianu, 2010).

Det viktigaste gällande mobila BI-lösningar är att man kan använda sitt system genom molnet. Användningen av dessa tjänster kan minska utgifterna för företag, öka flexibiliteten, öka tillgängligheten till systemet, men framförallt gör detta så att man inte behöver lagra några data lokalt på enheten utan bara använda sig av en klient kopplad till BI-tjänstens server (Power, 2013). Även Jackson (2011, se Power, 2013) menar att, om man utvecklar dessa tjänster på ett lämpligt sätt så ökar systemets pålitlighet.

3. Teoretiskt ramverk

Detta avsnitt syftar till att beskriva den teori som uppsatsen vilar på. Avsnittet kommer behandla säkerhet i mobila enheter utifrån de teman vi har specificerat. Den första delen av avsnittet kommer således att handla om säkerhet i mobila enheter generellt för att ge en bredare förståelse för detta område. Vi kommer sedan gå ner på en mer detaljerad nivå av säkerhet och analysera den mänskliga faktorn och policies/BYOD och hur dessa aspekter påverkar säkerheten i mobila enheter som används i företag.

3.1 Säkerhet i mobila enheter

Den ökade användningen av mobila enheter i företag har lett till att synen på hur arbetet ska utföras har förändrats, genom att anställda kan vara lika produktiva utanför kontoret som de är på kontoret. Den ökade mobila användningen leder till att anställdas förmåga att komma åt företagets information överallt och när som helst ökar, eftersom man inte längre är bunden till sitt kontor (Basole, 2007).

I och med att mobil teknologi ökar, ökar även risken med användning av dessa enheter. Det finns en mängd olika säkerhetsaspekter och risker som mobil teknologi kan medföra och det är en stor utmaning för företag att hantera mobila enheter, eftersom det inte finns någon standardlösning för hur man ska hantera de risker som detta medför (Rose, 2013). Rose (2013) delar upp riskerna med mobila enheter i tre olika kategorier, som förklaras kortfattat nedan.

1. Fysisk säkerhet
Här behandlas risker med själva enheten i sig. När en mobil enhet lämnar organisationen har man inte längre kontroll över vad som händer.

2. Intern säkerhet
Denna kategori behandlar säkerhet på ett internt plan, och tar upp datasäkerhet och dataöverföring. (I och med vår avgränsning och att vi inte ämnar behandla denna typ av risk så analyserar vi inte dessa risker närmare).

3. Användarrelaterad säkerhet (användares kunskap och ansvar)
Organisationer måste ha policies som tar upp frågor om säker hantering och förväntningar på hur användarna använder sina enheter.

Om vi analyserar dessa risker i samband med vårt syfte och frågeställning kan vi se att den fysiska säkerheten som Rose (2013) tar upp hamnar under vårt första tema “Mänskliga

faktorn", medan den användarrelaterade säkerheten kan sorteras in under vårt andra tema "Policies/BYOD".

3.1.1 "Den mänskliga faktorn"

När en mobil enhet lämnar organisationen har man inte längre kontroll över vad som händer. Då fler mobila enheter används för att komma åt företagsdata och de anställdas arbete blir mer mobilt, ökar risken för potentiella förluster av data då anställda kan tappa bort sin enhet eller risken med att enheten kan bli stulen (Thomson, 2012).

Enligt Thomson (2012) förlorar företag mer och mer kontroll över vem som har tillgång till deras interna nätverk. Rose (2013) menar att lösningen på detta är att skapa restriktioner i form av en lista på alla enheter som har tillgång till det interna nätverket för att förhindra att obehöriga får åtkomst.

Wright et al (2011) skriver att den största nackdelen med mobila enheter i organisationer är dess säkerhetsrisk, och något så simpelt som att tappa bort en telefon kan nu för tiden skapa en stor säkerhetsrisk för företag. Författaren fortsätter skriva om kritiska risker, så som stöld och missbruk av företagsinformation och att dessa risker blir extra stora i och med mobila enheter. Riskerna blir än större om företaget inte har implementerat någon strategi för att hantera säkerhetsaspekter för mobila enheter.

Wright et al (2011) menar att lösenord inte är ett tillräckligt skydd för den information som återfinns på de mobila enheterna i händelse av stöld eller förlust. Man måste även kunna låsa eller radera innehållet på sin enhet från distans för att inte riskera att information hamnar i fel händer. Eftersom många även använder sin enhet privat så förespråkar Wright et al (2011) och Semer (2013) att enheten delas upp i två olika partitioner med två olika inloggningar, där den ena innehåller företagsinformation och den andra innehåller privat information. På detta sätt kan man göra det möjligt att radera företagsinformationen utan att den privata informationen går förlorad.

3.1.2 Policies/BYOD

Praktiken "Bring Your Own Device" (BYOD) innebär att anställda tar med och använder sig av egna/privata enheter på jobbet, vilket många företag idag har anammat. Området kring BYOD medför flera fördelar för både företaget och de anställda. För företagets del minskar omkostnaderna och man kan helt eller delvis eliminera kostnaderna för sin IT-infrastruktur. Vidare kan produktiviteten och de anställdas belåtenhet öka och man kan avlasta IT-avdelningens support-arbete. Fördelarna för de anställda är att de fritt kan välja vilken enhet

de vill använda på jobbet, vilket kan öka arbetsmoralen. Det blir även färre enheter att bära runt på eftersom man använder den enhet som man ändå alltid har med sig (Semer, 2013; Zielinski, 2012). Zielinski (2012) skriver att i kontrast till de positiva sidorna med BYOD, finns det även risker med att använda sig av egna enheter på jobbet. En risk som nämns är om anställda lämnar organisationen men fortfarande har känslig data på sina enheter. En annan risk handlar om nedladdning av olagligt material, är det då användaren som blir skyldig eller är det organisationen som personen är anställd på som får ta smällen? Det är viktigt att chefer och HR-avdelningen förstår dessa risker innan man anammar BYOD i sin verksamhet (Zielinski, 2012).

I och med en ökad användning av egna enheter på arbetsplatserna måste företag förhålla sig till ständigt förändrade lagar, standarder och riktlinjer gällande datasäkerhet (Chaudhry, 2012). De som använder sina egna enheter i arbetet tar inte bara med sig hårdvara utan de tar även med sig sina egna applikationer, detta benämns som *Bring Your Own Application (BYOA)* (Chaudhry, 2012) eller *Consumer IT used as corporate IT* (Hudson, 2012). Användarna har med största sannolikhet några speciella verktyg som de föredrar att använda vid t.ex. delning av filer, exempelvis Dropbox. Om detta används har företaget inte längre någon kontroll över vem som har tillgång till dessa filer om användaren t.ex. delar sin Dropbox-mapp med någon annan (Chaudhry, 2012). För att komma underfund med dessa typer av problem behöver företag skapa en policy rörande BYOD, där en mobile device management (MDM) strategi kan inkluderas. En MDM-lösning är en "best practice" som installeras på enheten, vilken hjälper organisationen att reglera säkerheten och behålla kontrollen, även om de anställda använder sina egna enheter i arbetet. Denna typ av lösning gör det möjligt för företag att upprätthålla sina policies (Semer, 2013). Om de anställda skriver på ett avtal och godkänner att företaget installerar en MDM-lösning på enheterna, kan det i bästa fall skapas en balans mellan företagssäkerhet och de anställdas bekvämlighet då de får använda sina egna enheter (ibid).

Som tidigare nämnts förespråkar Wright et al (2011) och Semer (2013) att enheten delas upp i två delar, en del för privat bruk och den andra för arbete. I och med detta föreslår Semer (2013) att följande policies tillämpas:

- ***Anti-malware and firewall policy.*** *Mandates installation of security software to protect the device's apps, content, and operating system.*
- ***App/operating system update policy.*** *Requires devices to be configured to receive and install software updates and security patches automatically.*

- ***App-vetting policy.*** *Ensures that only trustworthy "white listed" apps can be installed; blocks "black listed" apps that could contain malicious code.*
- ***Encryption policy****. Ensures that the contents of the device's business container are encrypted and secured.*
- ***PIN policy.*** *Sets up PIN complexity rules and expiration periods, as well as prevents reuse of old PINs.*
- ***Inactive-device lockout policy.*** *Makes the device inoperable after a predetermined period of inactivity, after which a PIN must be entered to unlock it.*
- ***Jail break policy.*** *Prohibits unauthorized alteration of a device's system settings configured by the manufacturer, which can leave devices susceptible to security vulnerabilities.*
- ***Remote wipe policy.*** *Erases the device's business container contents should the device be lost or stolen.*
- ***Revoke access policy.*** *Disconnects the employee's device from the organization's network when the MDM's remote monitoring feature determines that it is no longer in compliance.*

(Semer, 2013 s. 25).

I likhet med Semer (2013) skriver även Rose (2013) om åtgärder som företag kan ta för att säkerhetsställa användningen av de mobila enheterna på företaget. Rose (2013) menar att:

- *Use device tracking software to know the location of all devices at all times.*
- *Keep an inventory of all mobile devices (both personal and organizational) permitted to access the organization's network.*
- *Use encryption on all devices with the capability.*
- *(...)*
- *Scan mobile devices routinely to ensure the latest updates and software versions are present.*
- *Provide continuous training and user expectation for the proper use of mobile devices.*
- *Create, review, and update mobile device policies and procedures regularly.*

(Rose, 2013 s. 48).

Som vi ser ovan så finns det några punkter som belyses av både Rose (2013) och Semer (2013). Dessa punkter handlar om kryptering av data på enheterna och uppdatering av den senaste mjukvaran. Där utöver behandlar båda författarna ett antal ytterligare punkter som de anser viktiga för företag att ha i beaktning när man hanterar mobila enheter.

Chaudhry (2012) menar att företag som inte anpassar sig till faktumet att anställda tar med sig sina egna enheter kan få betala ett högt pris då riskerna ökar. Om ett företag inte implementerar en policy så kommer de anställda automatiskt att skapa egna regler för användningen av enheterna i arbetet. Därför blir det absolut nödvändigt för företag att agera korrekt och i ett tidigt skede.

4. Metod

Vår studie har genomförts i samarbete med företaget Optivasys som uteslutande arbetar med BI-verktyget QlikView. Företaget har tillhandahållit kontakter med kunder och säljare som vi har intervjuat, vi har således haft god access till respondenter.

Vårt syfte med undersökningen har varit att undersöka viktiga säkerhetsaspekter med mobila BI-lösningar hos företag. Genom att kombinera tidigare studier om policies kring BYOD med studier kring hur mänskliga faktorer kan påverka säkerheten, har vi skapat vårt ramverk som vi har använt för att bygga vår intervjuguide (se bilaga 1 och 2). För att kunna studera säkerheten inom mobila BI-lösningar så har vi valt att avgränsa oss mot en specifik lösning (se avsnitt 4.1). Vår studie är en kvalitativ, tolkande studie (Walsham, 2006) och vår främsta datainsamlingsteknik var intervjuer.

Enligt Patel och Davidson (2011) är syftet med kvalitativa studier att få en djupare kunskap än den man får genom kvantitativa metoder. En fördel med kvalitativ analys är att man som forskare får en stor inblandning i den studie man utför, vilket ger en bra insikt i studiens händelser och dess aktörer.

Det finns inte bara fördelar med kvalitativ analys och kvalitativ data, det finns även ett flertal problematiska egenskaper med denna typ av metod. Kvalitativ data generar ofta mycket text, vilket kan leda till att klarheten i analysen kan försvinna när man summerar den (Cornford & Smithson, 2006).

Genom att intervjua kunder som använder sig av QlikViews mobila lösning har vi kunnat skapa oss ett trovärdigt resultat, då vi har fått en verklighetsbaserad bild av företags inställning till området i fråga. För att ge läsaren en bra överblick över det empiriska resultat vi genererat under vår undersökning, presenterar vi centrala delar av intervjuerna i form av citat kombinerat med kommenterande text. Patel och Davidsson (2011) menar att en sådan text bör innehålla en väl avvägd balans mellan citat och kommenterande text så att analysen inte överlåts åt läsaren.

4.1 Fallstudieobjekt; "QlikView"

QlikView[1] är ett BI-verktyg som kombinerar dynamisk presentation med realtidsanalys där man kan direktmanipulera data. Genom att använda QlikView kan användaren själv analysera olika typer av information, exempelvis försäljning, lager och framtida trender.

[1] http://www.QlikView.com/se/explore/experience/product-tour

QlikView kan användas på flera olika plattformar, däribland datorer och mobila enheter, systemet passar lika bra för större företag som för en enskild användare. Det område som QlikView verkar inom benämns som Business Discovery, vilken är en gren av Business Intelligence. Detta område är mer inriktat på att användaren ska "upptäcka" sin egen data, genom att själv kunna utföra analyser direkt i systemet och få omedelbar respons, i form av visuella presentationer såsom grafer och diagram. Det som skiljer QlikView från traditionella BI-system är att det inte genererar statisk information utan presentationen kan manipuleras direkt av användaren.

Med QlikView som fallstudieobjekt fick vi en grund att bygga våra intervjuer på. I och med detta så anser vi att vi fick mer trovärdiga svar, istället för att bygga vår studie runt en mer generell uppfattning om mobila BI-lösningar.

4.2 Intervju

För att få en bra uppfattning om hur företag ställer sig till de säkerhetsaspekter som undersökningen behandlar, beslöt vi oss för att göra intervjuer med användare av QlikView och även säljare av systemet. Anledningen till att vi intervjuade säljare av systemet var att få ett ytterligare perspektiv på vår frågeställning och en generell bild av hur kunder tänker kring säkerhetsaspekter.

För att få en bättre förståelse för vårt empiriska resultat och för att underlätta analysen har vi spelat in och transkriberat våra intervjuer. Walsham (2006) menar att en transkriberad intervju ger många fördelar för forskaren, bl.a. kan man fokusera mer på att få en bra kontakt med personen som intervjuas och då intervjun är transkriberad ges möjligheten att plocka ut exakta citat då man ska presentera sitt empiriska resultat. Nackdelarna med denna metod är, enligt författaren, att intervjupersonen kan känna sig obekväm och svara på frågorna på ett oärligt sätt samt att själva transkriberingen är tidskrävande.

Vi lade upp intervjuerna på ett semistrukturerat sätt (Patel & Davidson, 2011). Strukturmässigt arbetade vi enligt trattekniken (ibid) där vi först tog upp intervjupersonens generella bild av QlikView och mobilt BI för att sedan gå in på våra två specifika teman som behandlar de säkerhetsaspekter som vi undersökte, dvs.; *Policies kring användande av mobilt BI/Anställdas användande av privata enheter* och *Säkerhetsaspekter kring den mänskliga faktorn* (se bilaga 1 och 2 för intervjuguider).

Trattekniken innebär att man börjar med mer öppna frågor för att sedan leda in på mer specifika frågor. Denna teknik anses vara både motiverande och aktiverande (Patel & Davidson, 2011).

Enligt Patel och Davidson (2011) genomförs en semistrukturerad intervju genom att man gör en lista över de teman som ska beröras, och man ger intervjupersonen stor frihet att utforma svaren. Vidare behöver frågorna inte ställas i en bestämd ordning, vilket gör att intervjun har en låg grad av standardisering. Intervjuer klassificeras ofta utefter dess struktur, vilken sträcker sig från ostrukturerade till helt strukturerade intervjuer. Ostrukturerade intervjuer genomförs utan någon egentlig planering jämfört med strukturerade intervjuer där frågorna ställs i en speciell ordning, med endast korta förklaringar till frågorna. Ingen av dessa intervjuer lämpar sig för den form av studier som studenter genomför, utan här väljer man oftast semi-strukturerade intervjuer (Cornford & Smithson, 2006).

Cornford och Smithson (2006) menar att man genom intervjuer kan hantera mer komplexa områden än enkäter, i och med att intervjuaren kan justera sina frågor utefter intervjupersonen. Genom detta kan man addera frågor som man tycker är relevanta för stunden eller strunta i sådana frågor som känns irrelevanta. Författarna skriver vidare att intervjuer tillåter intervjuaren och intervjupersonen att ha en konversation, vilket kan leda till att oklarheter och missförstånd kan redas ut genom att någon av parterna kan förtydliga sitt svar eller sin fråga.

Vi började intervjuerna genom att ta upp frågor om mobilt BI och QlikView, för att få en övergripande bild av vad intervjupersonen anser om området. Vi fortsatte sedan in på mer specifika frågor om våra teman, där vi började med temat om policies och BYOD för att sedan gå in på temat om mänskliga faktorn. Typiska frågor vid intervjusituationerna var exempelvis:

- *Hur ser ni på tanken om ”Bring your own device”?*
- *Anser ni att det finns en risk att er företagsinformation hamnar i fel händer, ex. via borttappade/stulna enheter?*

Vi utarbetade två olika frågeformulär, ett för kunder och ett för säljare, detta för att samma typ av frågor inte passar in på båda grupper av respondenter (se bilaga 1 och 2).

För att ge det empiriska resultatet bättre validitet (Patel & Davidson, 2011) har vi även delat med oss av vårt empiriska material till Optivasys och låtit de läsa igenom och verifiera vårt resultat.

4.3 Urval

De kunder som vi har intervjuat fick vi tilldelat oss av Optivasys. På grund av tidsramen hade vi inte möjlighet att välja ut personer för intervju, utan vi fick intervjua de som fanns tillgängliga vid tiden för studien. Vi anser att detta inte har påverkat vårt resultat, i och med att vårt fokus för intervju låg på att hitta kunder som använder QlikView generellt och QlikView mobilt i synnerhet. De kunder vi har intervjuat använder QlikView mobilt, vilket vi anser ger bra data för vår studie. Den säljaren och den projektledare vi intervjuade valde vi baserat på deras stora kontakt med kunder då de har inblick i hur kunder tänker kring dessa säkerhetsaspekter.

4.3.1 Presentation av urvalsgruppen

Här följer en kort presentation av de informanter vi har intervjuat, vilka i vår undersökning kommer vara anonyma.

Säljare: Säljare och har arbetat med QlikView i 7 år. Har kontakt med kunder dagligen.

Projektledare: Projektledare och till viss del utvecklare, har arbetat med QlikView i 6,5 år. Har väldigt mycket kundkontakt.

Kund 1: IT-strateg på ett medelstort företag. Har god erfarenhet av QlikView och IT i stort.

Kund 2: CIO på ett internationellt företag. Har använt QlikView sedan 2006-2007.

I och med informanternas erfarenhet inom området, anser vi att samtliga informanter är trovärdiga källor att bygga vår fortsatta analys på.

5. Empiriska Resultat

Vårt resultat från undersökningen har genererat två perspektiv på vårt problemområde. Det ena perspektivet tar upp säljarens/leverantörens synvinkel och generella bild på de säkerhetsaspekter som uppsatsen behandlar och det andra perspektivet är från kundens synvinkel. Vi kommer i fortsättningen benämna *Säljare* och *Projektledare* som *säljare 1* och *säljare 2*. Detta för att framhålla att dessa är på leverantörssidan av QlikView. De två kunder vi har intervjuat kommer benämnas *kund 1* och *kund 2*.

Vi kommer i detta avsnitt visa på det resultat som framkom av intervjuerna, genom att presentera det material som är relevant i förhållande till vårt syfte och vår frågeställning. Materialet kommer att presenteras i form av citat och jämförelser mellan informanter och datan kommer presenteras utifrån de teman som vi presenterade tidigare i uppsatsen.

5.1 Generellt om mobila BI-lösningar

Enligt de säljare vi har intervjuat använder cirka 5 procent av deras kunder den mobila lösningen av QlikView, dock nämner informanterna att genom den kundkontakt de har så ser de en ökning inom området.

> *"Alla pratar nästan om det men det är inte så många som använder det"* (säljare 1).

> *"Men som sagt, jag tror fortfarande att man är...man är inte riktigt mogen för det tror jag inte hos företagen. Produkten i sig tycker jag är det, men efterfrågan är inte så enorm än, det är den inte, men det börjar komma mer och mer"* (säljare 2).

En av informanterna nämner det kritiska i att företag är med i utvecklingen av mobila enheter framöver, eftersom många pratar om det förutspår informanten att mobila enheter kommer att ta över i framtiden.

> *"Det kommer ju bara att explodera tror jag så att det är viktigt att va med där"* (säljare 1).

På frågan om kunders inställning till den mobila QlikView-lösningen framkom det att uppfattningen om de mobila lösningarna har förändrats med tiden.

> *"För tidigare har det varit lite: Ah, men det är en häftig grej men ah, men man har inte riktigt sett nyttan med det [...] allting har väl en mognadsprocess av sig självt så*

att säga. Så nu är det inte den där häftiga grejen längre utan nu är det faktiskt något som man kan ha nytta av" (säljare 2).

På frågan om varför kunderna anskaffade den mobila QlikView-lösningen svarar de följande:

"Absolut det var bara en idé som jag har drömt om länge att man kan få ut, få ut sådana här saker i...helst i telefonerna då" (kund 1).

"Ja alltså, det har ju bara att göra med att den information som företagsledningen bedömer som väsentlig, den ska man ju alltid ha tillgång till om man är i en beslutsfattande position för det är ju framförallt lite högre befattningar i organisationen som får mobilitet. Och där ska man alltid vara medveten, Know Your Numbers, som man säger i näringslivet. Det är lite granna samma sak här" (kund 2).

Det som har varit en bidragande orsak till företags skepsis mot mobila enheter i arbetet är enligt en av informanterna de konservativa IT-avdelningarna.

"Så det gäller nog att hitta de personerna som är lite framtidstänkande. Det är ju många IT-avdelningar som är rätt konservativa så att det gäller att hitta verksamheten som driver det här lite hårdare" (säljare 1).

En av kunderna nämner också att detta kan vara en bidragande orsak.

"Jag tror att både till IT-chefer, traditionell IT drift så absolut, de tycker säkert det här är jättejobbigt att förhålla sig till va. Det ligger väl någonstans i den rollens natur också att man ska tycka det. Det är en viktig fråga" (kund 1).

En av säljarna tar, i enlighet med kund 2, upp en aspekt av varför dessa framtidstänkande personer anskaffar den mobila QlikView-lösningen.

"Tillgänglighet är den största aspekten då att man ska komma åt den även om man är ute på vägarna, och enkelheten då. Att istället för att behöva ladda ner någonting på pc och liknande, att hela tiden kunna få det upp lite snabbare då.
Så det är ju en del, sen är det ju som sagt att säkerhetsfrågan är ju en viktig del i det här och den kan ju vara en ganska stor bromskloss från IT:s sida" (säljare 1).

Efter att ha fått en generell uppfattning av säljarnas och kundernas inställning till mobila enheter och den mobila QlikView-lösningen i synnerhet, fortsatte vi in på området kring

säkerhet och vad informanterna har för inställning till det. För att leda in på ämnet frågade vi om deras generella uppfattning kring säkerhetsfrågor. Säljarna fick frågan om säkerhetsaspekter är någonting som kunderna har frågor om.

> *"Ja som sagt jag tror att det är den största bromsklossen när det gäller den här utvecklingen och det är framför allt IT* (IT-avdelningen) *då som stoppar, liksom: det här blir en säkerhetsrisk"* (säljare 1).

En av kunderna är inne på samma spår som säljare 1 när det gäller inställningen till säkerhet.

> *"[...] säkerheten är ett bekymmer, ingen tvekan om det. Det vet man ju folk tappar bort sin PC och…sådant förekommer ju va och då kan det ligga data på den och så, nä så det är bekymmersamt"* (kund 2).

I och med att de säljare vi har intervjuat har kontakt med olika kunder så skiljer sig deras uppfattning åt. Till skillnad från säljare 1 så anser säljare 2 att kunders inställning till säkerhet har förändrats.

> *"[...] man har tyckt att det har varit för stor risk och ha liksom den här typen av verktyg, men nu börjar man förstå att så jädra farligt är det inte, kanske som man ändå har tänkt sig att det har varit en gång i tiden"* (säljare 2).

Båda kunderna är medvetna om att säkerheten är ett problem, men de anser att det egentligen inte är någon skillnad mot den information som man har på exempelvis sin mail.

> *"[...] det är väl en av anledningarna till att vi inte har gjort det* (använda de mobila applikationerna utanför brandväggen) *hittills, det är just säkerhets... säkerhetsaspekterna, hur...jag skulle aldrig ställa en QlikView-server utanför firewallen till exempel, det känns jävligt lurigt [...] fan du har så mycket annat i telefonen som ändå, som fuckas upp då alltså, ditt mailkonto och allt...nu kan man visserligen styra det från mailservern men ändå, så att...jag vet inte, men det är helt klart något att förhålla sig till"* (kund 1).

> *"[...] många personer i ledande befattningar har sin mail här till exempel och där kan det stå mycket information som kan vara väldig lättillgänglig om man råkar tappar bort den"* (kund 2).

De säljare vi har intervjuat anser att riskerna inte är särskilt stora och att nyttan ofta överväger riskerna. Kunderna däremot har lite olika åsikter kring detta, vilket kan bero på att det är två olika typer av företag där de kunder vi har intervjuat har något olika roller. Eftersom det mobila området är relativt nytt är det naturligt att ett visst motstånd uppstår men alla informanter är överens om att detta är ett fenomen vi kommer att se mer och mer av i framtiden.

5.2 Policies och BYOD

De säljare som vi har intervjuat har något olika syn på området BYOD. Säljare 1 tycker att BYOD är en väldigt bra idé eftersom man är van vid den typ av enhet man använder utanför arbetsplatsen.

> *"[...] men eftersom vi går lite mot att, varför kan vi inte ha det lika enkelt på jobbet som vi har det hemma, jag är van med Apple eller jag är van med PC, varför ska jag lära mig det här? Så jag tror ju att det kommer bara bli större och större och det ser man ju i USA där det både börjar och utvecklas mest så att säga, så att det kommer till Sverige snart"* (säljare 1).

Kund 1 är enig med säljare 1.

> *"Jag tycker det är suveränt, om det gör att jag presterar mer så absolut. Säkerheten får man hantera på något vis ändå i det hela men...jag ser inget fel med det. Sen beror det lite på vad det är för typ av arbetsplats"* (kund 1).

Säljare 2 angriper frågan mer från ett kundperspektiv och nämner följande om BYOD:

> *"[...] den lilla skaran som just nu är aktuell för att använda alltså mobilitet och så vidare, då ser man till och köpa in iPads eller...oftast så sitter ju de redan på företagets telefoner så att säga, men ledningsgrupp och VD och säljchef och så vidare, de kommer ju inte dit med sina egna telefoner kanske"* (säljare 2).

Kunderna bekräftar det som säljare 2 säger.

> *"[...] jag tror inte det är jättevanligt att man har med sig egna...det är väl någon iPad här och var som man ser, som någon har med sig, men generellt sett så är det vi som tillhandahåller hårdvaran då om man säger"* (kund 1).

"Alltså företaget tillhandahåller ju generellt enheter men det finns ju, jag menar jag kör ju hemifrån med min hem-PC mot företagets nät via VPN" (kund 2).

Sammanfattningsvis kan vi slå fast att de kunder som använder sig av de mobila lösningarna av QlikView ser till att köpa in de enheter som systemet kommer att användas på men det förekommer även privata enheter. Säljare 2 nämner att när det fortfarande är i ett test-stadie så finns det kunder som använder det på sina privata enheter, men de som ska använda det i större skala köper in enheter.

"Däremot så vet jag att det finns lite mindre kunder kanske som mer, aja men då kan jag testa med min enhet jag har hemma liksom, och så öppnar man upp en VPN-anslutning och så är det 'fine' med det. Men då är det ju mer kanske på ett test-stadie fortfarande än faktiskt något de använder" (säljare 2).

När vi nu har fastslagit vad de tillfrågade säljarna och kunderna anser om BYOD, fortsätter vi in på området kring policies. På frågan om de tyckte att man som företag ska ha en formell policy med avseende på mobila enheter, svarar säljarna följande:

"Ja det är nog ett måste, både ur revisionsvinkel och allt från olika certifieringar och annat så behöver man ju ha en policy sen är frågan hur mycket den följs, det är nog olika för olika bolag" (säljare 1).

"Ja, det tycker jag nog att det är. Sen är det väl det nog kanske inte specifikt mobila enheter, utan det är nog generellt [...] Alltså så att, det tycker jag nog mer hänger ihop med generell policy snarare än något mobilt, jag känner inte att det är så unikt för det. Men självklart så tycker jag att det bör finnas policies för hur man får använda den" (säljare 2).

På frågan om företaget använder sig av formella policies svarar kunderna olika. Kund 1 svarar att de inte har någon formell policy alls, men säger att det är viktigt att upprätta om användningen av mobila enheter ökar. Kund 2 använder sig av policies och anser även att det är viktigt.

"Ja det tycker jag, det har vi. Det ska inte överdrivas men vi har policies som folk får skriva på vi har ett gäng dokument med en informationssäkerhetspolicy överst som företagsledningen hanterar och sen har vi då dokument som jag som PC-användare

får skriva på och det tycker jag är viktigt. Och det får alla som kommer hit, och då får de kvittera, läst och förstått att de kommer följa de här reglerna" (kund 2).

Enligt säljare 1 så verkar de policies som används ute i vissa organisationer vara utdaterade och inte specifika för de mobila enheterna som används. För att lösa detta föreslår säljare 1 följande:

"[...] jag tror det svåra med det här är ju att tekniken förändras ju så väldigt de här senaste åren och policiesarna ligger ju kvar, som sagt vi har gjort vid någon typ av certifiering för 7 år sen, så en uppdaterad policy eller en levande policy är nog att rekommendera eftersom att på 2, 3 år så är det ju både nya verktyg och nya möjligheter va att, men det är ju självklart att man kan ju inte släppa allting fritt utan det är ju bra att en organisation har en policy att luta sig mot så att de inte kan bli överkörda av någon i organisationen" (säljare 1).

Vidare föreslår säljare 1:

"[...] beroende på vad det är för typ av information så får man ju ha olika regler för de olika informationerna. Det kan ju vara så att i många fall finns det ju möjlighet att ladda ner QlikView-applikationer och ta med sig kanske försäljningsdata med en viss begränsning, du får bara köra det med lite mer högrisk information på jobbet och innanför nätverket" (säljare 1).

En sådan levande policy ska, enligt säljare 1 innehålla ganska konkreta delar så att de kan känna sig komfortabla att besvara frågor gällande användningen av de mobila enheterna. Säljaren anser även att det är ännu viktigare på större företag där en viss byråkrati behövs.

Vi frågade även kunderna vad de anser är viktigt att ha med i en formell policy. Där svarade de följande:

"Tror att det hänger lite ihop med vilken typ av app det är, det vill säga hur...hur långt ner i någonting du kan komma. Egentligen att titta på ett affärsområdes resultat under ett pågående år, det kanske inte säger så mycket för ens en konkurrent" (kund 1).

"Ja det är ju framförallt säkerhetsaspekten som är viktig sen har vi väl lite ytterligare i den policyn men, att man sköter sig och inte tar risker ute på nätet framförallt. Och

självfallet att om man har företagets data på [...] telefonen med och på PC:n att man är försiktig med sin utrustning helt enkelt, att man har bra lösenord, till exempel kräver lösenordsbyte var trettionde dag" (kund 2).

5.3 Säkerhetsaspekter kring "den mänskliga faktorn"

Båda säljarna anser att det finns en viss risk med att ha tillgång till företagsinformation dygnet runt på en mobil enhet men detta beror helt på vilken typ av information som finns på enheten. Även om båda informanterna nämner att detta är en risk, så diskuterar de hur stor risken egentligen är.

> *"För jag tror ju mycket att den datan man väljer att publicera på det sättet, den går och få tag på något annat sätt om man verkligen vill [...] Samtidigt som man ska ha respekt för det, självklart. Men jag tror det finns andra sätt att få tag på samma information"* (säljare 2).

I likhet med säljare 2 anser kund 1 att det inte är någon större risk att anställda har tillgång till företagsinformation dygnet runt. Kund 2 anser däremot att detta är en risk att ta hänsyn till. Säljare 1 menar att, på samma sätt som det finns risker med att ta med sig informationen på sin mobila enhet, så har dessa risker även funnits historiskt.

> *"Men frågan är om historiskt sett när alla gick runt med sina PDF-rapporter i sin väska, det var nog lättare att tyda det än att komma in i en iPad"* (säljare 1).

På frågan om riskerna med att de mobila enheterna hamnar i fel händer, dvs. då man tappar bort eller blir bestulen på sin enhet, svarar säljarna följande:

> *"[...] om man tappar bort de* [mobila enheterna] *så är det ju ganska liten chans att det hamnar i orätta händer och att den informationen ska vara viktig för den personen som stjäl den är nog ganska minimal"* (säljare 1).

> *"[...] och som sagt, att det* [informationen] *av en slump skulle hamna i händerna på någon som använder den typen av information på ett felaktigt...alltså jag vet inte, jag tycker det är lite långsökt"* (säljare 2).

Säljare 2 tror även att kunderna ser detta på samma sätt.

”Nja, jag tror...det korta svaret är nog nej. Att...i så fall så hade de nog inte infört det. Däremot så kan det nog finnas olika anledningar till varför svaret är nej, och det ena är nog att det finns de som faktiskt har resonerat kring det och så finns det de som; Äh, skit samma, alltså man ser...man har lite förbisett det och kanske inte tyckt att det är så himla noga” (säljare 2).

Kund 1 nämner att det är en risk, men hur stor risken är beror på vilken typ av information som finns i den mobila applikationen.

”[...]det beror lite på hur, vad som exponeras i de här apparna, men självklart har du en riktig, en riktig nitty-grittygrej som går ner på liksom transaktionsnivå eller inne i reskontror eller kunddatabaser och så vidare så är det klart att det finns en risk, definitivt det gör det” (kund 1).

Även kund 2 är fullt medveten om att risken finns.

”Det finns en sån risk, ingen tvekan om det[...]det är ingen behaglig situation, men vi har aldrig varit ute för några jätteallvarliga incidenter så här långt i alla fall och det är ändå baserat på ganska många års användning. Men det är ju klart att vad som händer imorgon vet man ju aldrig [...] det här är en stor risk, det är svårhanterligt och det kommer ständigt nya utrustningar ni vet det kommer paddor och nästa vecka kommer nått annat och det är svårt att hänga med i dom här svängarna” (kund 2).

Om en enhet tappas bort eller blir stulen så finns det säkerhetsåtgärder att vidta i QlikView. Säljare 1 fokuserar på datasäkerheten i sitt svar och nämner följande:

”Det som är bra med QlikViews lösning är ju att all information finns ju på servern, så om du tappar bort en iPad, så kommer du ju inte åt... så kommer du ju inte åt den informationen utan lösen och inloggningsuppgifterna då” (säljare 1).

Säljare 2 däremot, fokuserar till större del på andra säkerhetsåtgärder.

”[...] det finns ju en full-licens-modell och så finns det ju en dokument-licens-modell. Har du dokument-licens-modellen så kan du ju faktiskt plocka bort den licensen [...] Och sen finns det ju, alltså det som, så att säga, ligger utanför QlikView som självklart kanske då stryka VPN-åtkomst eller något annat för den enskilda användaren och sådana här saker. Men just i QlikView så handlar det ju mer om då

kanske och plocka bort en licens eller stryka mobil-åtkomsten helt på de applikationerna så att säga" (säljare 2).

På frågan om kunderna har säkerhetsåtgärder att vidta när en anställd tappar bort sin mobila enhet, svara båda informanterna att det finns rutiner för detta, genom att från distans slå av eller rensa telefonen.

För att sammanfatta intervjuerna frågade vi informanterna om de säkerhetsaspekter vi belyst skulle kunna påverka företags beslut att anskaffa den mobila QlikView-lösningen, vilket det råder delade meningar om.

"Nej, inte för fem öre. Det skulle det inte. Alternativet är ju att folk skickar siffror, eller vad det nu är man skickar, i Excel och det ena med det andra och man har ju sin mail så då är det ju ändå där så att, nej det påverkar inte" (kund 1).

"Det tror jag säkert, det är jag övertygad om [...] Vi kan sitta här på IT-staben och säga: Vi har policies, vi ska inte ha paddor, vi ska inte ha det, vi ska inte ha detta men det håller aldrig. Går det en tid så kommer det ändå va, och det kanske är rätt också, det kanske är vi som ska då försöka hänga med på säkerhetssidan och uppdatera och klara detta va. Men vi är ju naturligtvis lite motsträviga, det är vi" (kund 2).

"Ja absolut, jag tror att det är den största fördomen att mobila klienter och liknande ska vara en stor säkerhetsrisk. Så det är nog även en politisk fråga men även ett konservativt tänkande" (säljare 1).

"[...] jag tror fortfarande att säkerhetsfrågan är någonting som ligger och gnager. Det tror jag. Och, jo men det är nog faktiskt den övervägande delen fortfarande. I kombination då med vilken nytta man faktiskt får ut av lösningarna, alltså hur mycket man tycker det är värt och släppa ut den, så att säga, kontra vad man faktiskt får ut av den" (säljare 2).

6. Diskussion/Analys

Syftet med vår uppsats var att undersöka om och hur säkerhetsaspekter spelar in i ett företags beslut att anskaffa mobila BI-lösningar. Genom att kombinera tidigare teorier inom området med våra empiriska resultat, har vi skapat oss en grund för vår diskussion och analys. Vi kommer att diskutera det viktigaste resultatet av de aspekter vi har undersökt för att finna ett svar på vår frågeställning.

Som visats i det empiriska resultatet är samtliga våra informanter medvetna om att det finns risker då mobiliteten i företag ökar. Dessa risker ökar då anställda i organisationer tar med sig sina egna privata enheter och använder för att komma åt företagsdata. I likhet med Rose (2013) har våra informanter insett att riskerna eskalerar då fler mobila enheter äntrar organisationen och får tillgång till företagsdata. Trots denna medvetenhet, är detta ingenting som har stoppat de kunder vi intervjuat från att använda den mobila lösningen av QlikView. Enligt Semer (2013) och Zielinski (2012) finns det flera fördelar med BYOD. En av fördelarna är att produktiviteten och anställdas belåtenhet kan öka vilket även till viss del framkom i vår empiri, genom att flera av informanterna är positiva till BYOD och anser att utvecklingen går mot att man vill ha det lika enkelt på jobbet som man har det hemma. Samtidigt framkom att detta inte är något som egentligen tillämpas hos de kunder vi intervjuat då de till stor del ser till att köpa in enheter till sina anställda.

Oavsett om företaget tillhandahåller enheter till personalen eller om de tar med sig sina egna, så förekommer det att enheterna följer med de anställda utanför organisationen. I likhet med Rose (2013) och Thomson (2012) visar vår undersökning på att det finns en liten risk med att enheter lämnar organisationen då de tas med hem efter arbetstid. Den risk som uppstår i och med att enheten tas hem efter arbetstid är att den kan tappas bort eller bli stulen. Som Wright et al (2011), Rose (2013) och Thomson (2012) antyder, är borttappade och stulna enheter en stor säkerhetsrisk. Enligt vår undersökning anses denna risk inte vara fullt så stor som teorin beskriver. De informanter vi har intervjuat anser att det finns en viss risk med borttappade och stulna mobila enheter, men riskens omfattning beror på vilken typ av data som exponeras. De nämner även att det är en mycket liten risk att dessa data hamnar i fel händer och att mycket av den informationen går att hitta på annat håll. Till skillnad från de övriga informanterna, anser en av de intervjuade att detta är en stor risk och att det är en svårhanterlig situation. En anledning till att de flesta informanter inte ser detta som en stor risk, kan förklaras på samma sätt som säljare 1 beskrev problemet.

> *"Men frågan är om historiskt sett när alla gick runt med sina PDF-rapporter i sin väska, det var nog lättare att tyda det än att komma in i en iPad"* (säljare 1).

Detta anser vi kan vara en av de största orsakerna till att risken med borttappade och stulna enheter inte upplevs som så stor av de flesta informanter. I och med att mycket information som man idag har på mobila enheter även har funnits historiskt, men då i annan form, gör att denna risk alltid har funnits och inte beror på de mobila enheternas intåg i företagsvärlden.

Enligt ett par av informanterna finns det mycket information på mobila enheter, utöver den som finns i BI-applikationer, som kan vara känslig för företag och även mer lättillgänglig för personer som vill få tag i informationen. Informanterna tar upp att mailen är en sådan källa där känslig information återfinns.

Om en enhet blir stulen eller tappas bort är det viktigt att ha säkerhetsåtgärder. Wright et al (2011) och Semer (2013) diskuterar olika åtgärder att använda sig av när mobila enheter tappas bort eller blir stulna. En lösning som nämns är *remote wipe*, dvs. möjligheten att låsa eller radera innehållet på enheten från distans. Detta är en lösning som de kunder vi har intervjuat använder sig av i händelse av borttappade och stulna enheter. Säljarna fokuserar mer specifikt på möjligheter att blockera åtkomst i QlikView och nämner att man kan blockera tillträde för en viss licens och häva åtkomsten till servern och därmed all information.

Som Chaudhry (2012) skriver så är det viktigt för företag att sätta upp policies. I och med den ökade användningen av mobila enheter gäller det för företag att implementera en policy i ett tidigt skede, innan de anställda skapar sina egna regler för användandet. I vår empiri framkom en skillnad mellan de kunder vi intervjuade, då det visade sig att en av kunderna inte använder policies alls i dagsläget, men säger vidare att det är viktigt att införa om användandet av mobila enheter ökar. Den andra kunden använder däremot policies och anser att det är viktigt men att det inte heller ska överdrivas. I likhet med kunderna, anser även båda säljarna att det är viktigt att använda sig av policies, en av säljarna ifrågasätter dock hur mycket de egentligen efterföljs.

Som vi såg i teorin tar Rose (2013) och Semer (2013) upp ett antal olika policies som företag kan använda sig av i samband med användning av mobila enheter. Ett exempel på dessa policies är det som Semer (2013) tar upp, i form av en lösenords-policy. I denna policy ingår regler för utformning av lösenord och hur frekvent man ska byta ut sitt lösenord. Detta är även något som framkom genom intervjuerna, där en av kunderna framhöll att en sådan policy tillämpades. Vår studie visar att policies är viktiga och bör implementeras i organisationer där mobila enheter används, men att det beror på hur många användare det

gäller och vad det är för typ av information som hanteras i applikationerna. Om företaget använder sig av mobila BI-applikationer tycks det vara extra viktigt med policies, eftersom den information som hanteras i dessa applikationer ofta är känslig för företaget.

Chaudhry (2012) lyfter, som vi sett i teorin, fram vikten av att företag förhåller sig till förändringar i omvärlden, så som förändrade lagar, regler och standarder. I likhet med författaren nämner en av säljarna att en levande policy är att föredra, i och med att det sker kontinuerliga förändringar. Eftersom tekniken är i ständig utveckling och att förutsättningarna ständigt förändras, blir det svårt för företag att skapa en policy som håller sig aktuell.

Vår avslutande fråga i samtliga intervjuer var om informanten ansåg att de säkerhetsaspekter vi belyst skulle kunna påverka ett företags beslut att anskaffa mobila BI-lösningar. På denna fråga svarade tre av fyra respondenter att beslutet skulle kunna påverkas, ett svar som återspeglar den teori vi arbetat med. Vår undersökning visar på att säkerhetsaspekter påverkar beslutet, men inte i den grad att man beslutar att inte införa BI-lösningen. Om lösningen är tillräckligt bra så tycks det bara vara en tidsfråga innan den kommer införas ändå.

7. Slutsatser

De säkerhetsaspekter som diskuterats ovan ligger till grund för svaret på vår frågeställning: *Hur spelar säkerhetsaspekter in i ett företags beslut att anskaffa mobila BI-lösningar?*
Vår huvudsakliga upptäckt är att dessa säkerhetsaspekter är någonting som företag funderar kring och har i åtanke, men att de inte alltid anser att riskerna med mobila BI-lösningar är så stora att det påverkar beslutet att anskaffa dessa lösningar. De säkerhetsaspekter vi har presenterat är enligt vår undersökning inte specifika för de mobila BI-lösningarna, de är mer relaterade till den ökade användningen av mobila enheter.

En slutsats vi kan dra är att risken med borttappade eller stulna enheter anses vara relativt liten, även om det samtidigt anses vara en risk man bör ta hänsyn till och ha i åtanke. En anledning till varför denna risk kan uppfattas som liten framkom genom studien, nämligen att den information som återfinns i mail och i liknande program kan vara minst lika känslig. Det framkom även att risken att informationen skulle hamna i fel händer, i händelse av borttappade eller stulna enheter anses vara väldigt liten.

BYOD är ett fenomen som vi, de källor vi undersökt och våra informanter är övertygade om att vi kommer se mer av i framtiden vilket gör det extra viktigt att planera för dess intåg i företaget. Enligt vår undersökning är BYOD ett område som inte har vuxit sig så stort än, vilket gjort att riskerna som det kan medföra inte är något som man har börjat ta med i beräkningen. För att behålla kontrollen över enheterna är det viktigt för företag att införa policies. Enligt vår undersökning anses policies vara viktiga och någonting som företag bör använda sig av, speciellt när antalet enheter i organisationen ökar. Under undersökningen har vi sett en lösning på hur företag kan hantera de säkerhetsaspekter vi har diskuterat. Denna lösning handlar om det kritiska i att ha en levande policy, dvs. en policy som uppdateras med åren och som på så sätt kan hantera nya former av enheter, lösningar, tjänster och nya risker som uppstår i och med detta.

7.1 Begränsningar och förslag till fortsatt forskning

Vår undersökning är baserad på en specifik BI-lösning vilket gör att våra resultat inte nödvändigtvis representerar BI-lösningar generellt. I och med tidsbegränsningen var vi tvungna att avgränsa vår undersökning till ett fåtal informanter, vilket har lett till ett begränsat resultat. Med detta i åtanke anser vi att det behövs ytterligare forskning på området, där fler informanter deltar och andra BI-lösningar analyseras.

Vi föreslår att våra slutsatser kan användas som en grund i fortsatt forskning, där man kan analysera och undersöka hur olika säkerhetsaspekter spelar in beroende på typ av företag och typ av information som återfinns på företaget. Detta är något som har framkommit under vår undersökning men som vi, på grund av studiens omfång inte har kunnat undersöka närmare.

Något som man kan forska vidare kring är att från grunden analysera företags beslut och vilka säkerhetsaspekter som tas med i beräkningen vid anförskaffandet av mobila BI-lösningar. Vi har analyserat *hur* vissa säkerhetsaspekter har spelat in i företags beslut, i fortsatt forskning kan man mer fokusera på *vilka* säkerhetsaspekter som faktiskt spelar in.

Källförteckning

Airinei, D. & Homocianu, D. (2010) The Mobile Business Intelligence Challenge, *Economy Informatics*, 10(1), 5-12.

Basole, R. (2007) The Emergence of the Mobile Enterprise: A Value-Driven Perspective, *Sixth International Conference on the Management of Mobile Business,* (ICMB 2007).

Chaudhry, P. (2012) Needed: a corporate mobile device policy*, Financial Executive; Morristown,* 28(5), 69-70.

Cornford, T. & Smithson, S. (2006) Project Research in Information Systems, *Palgrave Macmillan*.

Hudson, D. (2012) Managing Entrepreneurial Employees Who Bring Their Own IT to Work. *Technology Innovation Management Review*, December 2012:6-11.

Kuntze, N., Rieke, R., Diederich, G., Sethmann, R., Sohr, K., Mustafa, T. & Detken, K. O. (2010) Secure mobile business information processing, *Embedded and Ubiquitous Computing (EUC)*, 2010 IEEE/IFIP 8th International Conference on (s. 672-678). IEEE.

Lawton, G. (2006) Making business intelligence more useful, *IEEE Computer Society*, 39(9), 14-16.

Negash, S. (2004) Business intelligence, *Communications of the Association for Information Systems*, 13(1), 177-195.

Oberheide, J., Veeraraghavan, K., Cooke, E., Flinn, J. & Jahanian, F. (2008) Virtualized in-cloud security services for mobile devices, *Proceedings of the First Workshop on Virtualization in Mobile Computing* (s. 31-35). ACM.

Patel, R. & Davidson, B. (2011) Forskningsmetodikens grunder - Att planera, genomföra och rapportera en undersökning, *Lund: Studentlitteratur AB*.

Popovič, A., Hackney, R., Coelho, P. S. & Jaklič, J. (2012) Towards business intelligence systems success: Effects of maturity and culture on analytical decision making, *Decision Support Systems*, 729-739.

Power, D.J. (2007) A Brief History of Decision Support Systems, *DSSResources.COM, World Wide Web, http://DSSResources.COM/history/dsshistory.html*, version 4.0, March 10, 2007.

Power, D. J. (2013) Mobile decision support and business intelligence: an overview, *Journal of Decision Systems*, 22(1), 4-9.

Rose, A.D. (2013) Mobile Devices: Know the Risks, Know the Safer Practices, *Journal of Health Care Compliance*, ISSN 1520-8303, 01/2013, 15(1), 47.

Semer, L (2013) Auditing The BYOD Program, *The Internal Auditor*, ISSN 0020-5745, 02/2013, 70(1), 23.

Stipic, A. & Bronzin, T. (2011) Mobile BI: The past, the present and the future. *In MIPRO,* 2011 Proceedings of the 34th International Convention (s. 1560-1564). IEEE.

Talati, S., McRobbie, G. & Watt, K. (2012) Developing business intelligence for Small and Medium Sized Enterprises using mobile technology, *Information Society (i-Society)*, 2012 International Conference on (s. 164-167). IEEE.

Thomson, G. (2012) BYOD: enabling the chaos, *Network Security*, 2012(2), 5-8.

Violino, B. (2012) A calculated risk: as mobile devices continue to flood into the enterprise, IT leaders grapple with ways to manage the risk.(FORECAST 2013), *Computerworld*, 46(17), 31-32.

Walsham, G. (2006) Doing interpretive research, *European Journal of Information Systems*, 15(3), 320-330.

Wright Jr, H. R., Mooney, J. L., & Parham, A. G. (2011). Your firm's mobile devices: How secure are they?, *Journal of Corporate Accounting & Finance*, 22(5), 13-21.

Zielinski, D. (2012) Bring Your Own Device - More employers are allowing employees to use their own technology in the workplace. *HRMagazine*, ISSN 1047-3149, 02/2012, 57(2), 71.

Bilaga 1 – Intervjuguide Kund

INTERVJU KUND

Intervjudata

Namn:	
Titel:	
Datum för intervju:	
Plats:	
Inspelningsdata:	
Genomförd av:	
Andra noteringar:	

Bakgrundsfrågor

- Vilken roll har du vid XXXX?
- Hur länge har du arbetat inom organisationen?
- Vilka är dina huvudsakliga arbetsuppgifter?

Övrigt, beroende på respondent:

Generella frågor om det övergripande fenomenet

- Varför skaffade ni just QlikView?
- Hur använder ni QlikView?
    - *Använder ni det mobilt?*

  Om informanten har mobil QlikView-lösning
  - Varför skaffade ni den mobila QlikView-lösningen?

- Vad var det som gjorde att ni började använda QlikView?
- Vad anser ni är de största säkerhetsriskerna då man använder BI på mobila enheter?

Övrigt, beroende på respondent:

Specifika frågor om fenomenet

Tema 1: Policies kring användande av mobilt BI/Anställdas användande av privata enheter

- Använder era anställda egna privata enheter i jobbet eller tillhandahåller företaget mobila enheter?
- Hur ser ni på tanken om ”Bring Your Own Device”?
- Har ni några regler/policies kring användandet av QlikView på mobila enheter?
- Är det viktigt att ha formella (nedskrivna) policies eller anser ni att det räcker med informella policies?

Om informanten har policies

- Hur ser dessa policies ut?
- Vad anser ni är viktigast att ha med i sådana policies?

Om informanten inte har policies

- Har ni haft tankar på att införa policies på företaget?
- Vad anser ni är viktigast att ha med i sådana policies?

- Finns det en säkerhetsrisk med att anställda har tillgång till informationen 24/7?

Tema 2: Säkerhetsaspekter kring den mänskliga faktorn

- Anser ni att det finns en risk att er företagsinformation hamnar i fel händer, ex. via borttappade/stulna enheter?

- Om en anställd tappar bort/blir bestulen på sin mobila enhet - hur agerar ni då? Finns det några säkerhetsåtgärder i sådana situationer?

- Har anställda möjlighet att spara inloggningsuppgifter för QlikView lokalt på den mobila enheten?

- Tror du att de risker vi har diskuterat skulle kunna påverka beslutet att anskaffa QlikView mobilt?

Övrigt, beroende på respondent:

Bilaga 2 – Intervjuguide Säljare

INTERVJU SÄLJARE

Intervjudata

Namn:	
Titel:	
Datum för intervju:	
Plats:	
Inspelningsdata:	
Genomförd av:	
Andra noteringar:	

Bakgrundsfrågor

- Vilken roll har du här på företaget?
- Hur länge har du arbetat inom organisationen?
- Vilka är dina huvudsakliga arbetsuppgifter?
- Vad har du för uppdrag?

Övrigt, beroende på respondent:

Generella frågor om det övergripande fenomenet

- Hur länge har du arbetat med QlikView?
- Hur går du till väga när du ska sälja in QlikView till kund? Vilka är dina främsta säljargument?
- Hur stor del av era kunder använder QlikView mobilt?
- Vad har era kunder för inställning till den mobila QlikView-lösningen?
- Hur är trenden när det gäller de mobila lösningarna av QlikView?
    - Ökar användandet eller håller sig kunderna till desktop-versionen?
- Hur tror du det kommer se ut i framtiden, är detta någonting som kommer bli mer populärt?
- Vilka anser du är de mest avgörande aspekterna för företag som anskaffar mobil QlikView? Vad är det som får kunderna att skaffa denna lösning?

- Vilka anser du är de största säkerhetsriskerna då man använder BI på mobila enheter?
- Har kunder frågor angående säkerheten i den mobila QlikView lösningen när ni säljer in systemet?

Övrigt, beroende på respondent:

Specifika frågor om fenomenet

Tema 1: Policies kring användande av mobilt BI/Anställdas användande av privata enheter

- Vad tycker du om området kring ”Bring Your Own Device”?
- Vad har era kunder för inställning till ”Bring Your Own Device”?

- Anser du att det är viktigt för kunder att ha formella (nedskrivna) policies?
- Vad anser du är viktigt för kunder att ha med i policies rörande BYOD?
- Vet du om era kunder har regler/policies kring användandet av QlikView på mobila enheter?
    - *T.ex om man får skriva kontrakt på att man bara får använda QlikView under arbetstid.*
    - *Om det inte finns formella regler eller om det endast finns informella.*

- Vet du om era kunder tillhandahåller enheter till sina anställda?
    - *Använder dessa kunder ändå egna enheter på jobbet?*

- Finns det en säkerhetsrisk med att företags anställda har tillgång till informationen 24/7?

Tema 2: Säkerhetsaspekter kring den mänskliga faktorn

- Anser du att det finns en risk att företagsinformation hamnar i fel händer, ex. via borttappade/stulna enheter?
    - *Hur stor risk anser du att detta är?*
    - *Hur ställer sig era kunder till den här frågan? Är det något de har nämnt?*

- Om en användare tappar bort/blir bestulen på sin mobila enhet - Finns det några säkerhetsåtgärder att använda sig av i QlikView i sådana situationer?

- Har användare möjlighet att spara inloggningsuppgifter för QlikView lokalt på den mobila enheten?

- Tror du att de risker vi har diskuterat skulle kunna påverka beslutet för företag att anskaffa QlikView mobilt?

Övrigt, beroende på respondent: