HÖGSKOLAN
I GÄVLE

AKADEMIN FÖR TEKNIK OCH MILJÖ
Avdelningen för industriell ekonomi, industridesign och maskinteknik

Kontroll över informationsspridning vid outsourcing av underhåll för säkerhetskritiska system

En fallstudie inom industrisektorn

2019

Maja Myr och Louise Törnell

Examensarbete, Grundnivå (kandidatexamen), 15 hp
Industriell ekonomi
Industriell ekonomi - Industrial Management and Logistics

Handledare: Lennart Söderberg
Examinator: Ming Zhao

Förord

Detta examensarbete är slutet på vår treåriga utbildning Industriell ekonomi - Industrial Management and Logistics på Högskolan i Gävle. Examensarbetet berör ett område som vi finner mycket intressant, vilket varit möjligt att studera med hjälp av flera företag i Sverige. Vi vill därför tacka deltagande respondenter för deras medverkan. Vidare vill vi tacka vår handledare Lennart Söderberg och vår examinator Ming Zhao för stöd under arbetets gång.

Abstract

Outsourcing of the maintenance activities related to safety-critical systems poses several challenges, where unauthorised access can lead to severe consequences in terms of data vulnerability and huge income lost. Companies can prevent the dissemination of information by managing security, which also contributes to economic and social sustainability. The purpose of the study was to investigate how organizations in the industrial sector deal with the issues of information dissemination in the outsourcing of maintenance activities related to safety-critical systems. To study the area, eleven companies have been interviewed where the results have been compiled in a cross-case analysis, which has been analysed against previous research. The study shows that there are several factors leading to an increased risk of undesired dissemination. Furthermore, the study has resulted in a model for managing control over the dissemination of information in the outsourcing of maintenance for safety-critical systems.

Keywords: Dissemination, Safety-critical systems, Maintenance, Outsourcing, Blockchain

Sammanfattning

Outsourcing av underhåll för säkerhetskritiska system innebär flera säkerhetsutmaningar, där obehörigt intrång kan leda till förlorade data, information och inkomst. Företag kan förebygga informationsspridning genom att hantera säkerhet, vilket även bidrar till ekonomisk och social hållbarhet. Syftet med studien var att undersöka hur organisationer inom industrisektorn hanterar informationsspridning vid outsourcing av underhåll för säkerhetskritiska system. För att studera området har elva företag intervjuats där resultatet har sammanställts i en cross-case analys, som analyserats mot tidigare forskning. Studien påvisar att det finns flera faktorer som leder till ökad risk för oönskad informationsspridning. Vidare har studien har resulterat i en modell för att hantera kontroll över informationsspridningen vid outsourcing av underhåll för säkerhetskritiska system.

Nyckelord: Informationsspridning, Säkerhetskritiska system, Underhåll, Outsourcing, Blockchain

Innehållsförteckning

1. Inledning 4

1.1 Problembakgrund 4

1.2 Syfte 6

1.3 Forskningsfrågor 6

2. Metod 7

2.1 Angreppssätt 7

2.2 Metodreflektion 9

3. Teoretisk referensram 11

3.1 Outsourcing 11

3.1.1 Underhåll 11

3.1.2 Outsourcing av underhåll 13

3.1.3 Leverantörsrelationer 13

3.2 Säkerhet 14

3.2.1 Informationssäkerhet 15

3.2.2 Säkerhet vid extern åtkomst 16

3.2.3 Säkerhetspolicy 16

3.2.4 Standard för informationssäkerhet 17

4. Resultat 19

4.1 Underhållsleverantör 20

4.2 Tillverkande företag 21

5. Analys 25

5.1 Underhållsleverantörer 25

5.1.1 Vilka är de kritiska faktorerna för att behålla kontroll vid outsourcing av underhåll för säkerhetskritiska system? 26

5.2 Tillverkande företag 28

5.2.1 Vilka är de kritiska faktorerna för att behålla kontroll vid outsourcing av underhåll för säkerhetskritiska system? 29

5.2.2 Hur kan de identifierade kritiska faktorerna hanteras i verksamheten? 31

6. Slutsats 33

Referenser 34

Bilagor 39

1. Inledning

Avsnittet presenterar en inledning till studiens problem, syfte och frågeställningar.

1.1 Problembakgrund

Senaste årtiondets förändringar på marknaden har inneburit ökad komplexitet vad gäller teknik, i syfte att möta sociala, ekonomiska och miljömässiga utmaningar (Globala målen, 2019; Santos, Mehrsai, Barros, Ataújo & Ares, 2017; Saunila, Nasiri, Ukko & Rantala, 2019). Teknisk utveckling medför förändringar i försörjningsskedjan, vilket påverkar säkerheten då allt fler aktiviteter integreras (Christopher, 2016; Vaidya, Ambad & Bhosle, 2018). Förändringarna har lett till utvecklandet av begreppet Industri 4.0, i syfte att möta marknadens krav och bevara konkurrenskraft (Chaim, Muschard, Cazarini & Rozenfeld, 2018). Industri 4.0 innebär fjärde industriella revolutionen och infördes av den tyska regeringen (Rojko, 2017; Vaidya et al., 2018) för att möjliggöra automatisering, decentralisering samt integrering av produkter och tjänster (Santos et al., 2017).

Industri 4.0 är kopplat till uttrycket Internet of Things (IoT), vilket syftar till ett världsomspännande nätverk av sammankopplade objekt som kommunicerar med varandra i realtid (Vaidya et al., 2018). Vidare har det bidragit till framväxten av säkerhetskritiska system (Jansen, 2017), vilket innebär ett system som påverkar människors hälsa, säkerhet och välfärd om det har nedsatt funktion eller slutar fungera (Laplante & DeFranco, 2017). Obehörigt intrång kan leda till skada för såväl medarbetare, organisation samt omvärld (Jansen, 2017), vilket påverkar ekonomisk och social hållbarhet (Bendovschi, 2015). Vidare innebär det att samtliga aktörer på marknaden bär ett ansvar för säkerhet (Jansen, 2017). Internet of Things möjliggör att analysera och bearbeta data i realtid, vilket skapar förutsättningar att lösa problem när experter från hela världen kan delta i underhållsarbetet (Hagberg & Henriksson, 2018). Underhåll innefattar korrigering av buggar i system, uppgraderingar, anpassning av system till nya krav och förbättrad prestanda. Underhållsprocessen är ständigt pågående och krävs under hela objektets livstid (Flodén, 2013).

Outsourcing av underhåll är en trend som har blivit allt vanligare (Ali-Marttila, Marttonen-Arola, Kärri, Pekkarinen & Saunila, 2017; Murthy, Karim & Ahmadi, 2015; Tidd & Bessant, 2014) då företag vill fokusera på kärnverksamheten och sänka kostnader (Mishra, Kumar, Sharma & Dubey, 2017). När underhåll av säkerhetskritiska system

outsourcas medföljer flera säkerhetsutmaningar, där företag kan arbeta proaktivt för att upptäcka hot och etablera riktlinjer (Jansen, 2017; Kaur & Sharma, 2017; Langfield-Smith & Smith, 2003). Företag måste finna tillvägagångssätt för att leda och hantera utmanande teknik, då digitalisering kan leda till problem, exempelvis vad gäller ägande av data när företag samverkar (Santos et al., 2017). För att minska risken för oönskad informationsspridning är blockchain en omtalad teknik som säkrar transaktioner mellan parter i ett affärsavtal (Skinner, 2016). Ökad digitalisering och automatiserade industrier bidrar till att säkerhetsrisker ökar kraftigt, exempelvis vad gäller informationsspridning (Pereira, Barreto & Amaral, 2017). Vidare ställer det krav på hög säkerhet där företag måste skydda data och information mot obehörigt intrång (Oesterreich & Teuteberg, 2016).

Litteratursökning har påvisat ett forskningsgap vad gäller informationssäkerhet vid outsourcing av underhåll för säkerhetskritiska system. Enligt Dhillon, Syed & Sá-Soares (2016) saknas forskning gällande informationssäkerhet när organisationer outsourcar aktiviteter. Traditionell outsourcing fokuserar på faktorer såsom huvudkompetens (Prajogo och Olhager, 2011), sänkta kostnader (Christopher, 2016), tillgång på extern kompetens, stordriftsfördelar och volymflexibilitet (Bengtsson, Berggren & Lind, 2005). Vid sökningar över publicerade artiklar i Scopus, IEEE Xplore och Science Direct:s databaser är tillgången begränsad. Kaur och Sharma (2017) påpekar att det krävs fortsatta studier för att hantera utmaningar som outsourcing medför gällande informationssäkerhet. Studien är en multipel fallstudie och baseras på ett flertal intervjuer, i syfte att undersöka hur industriföretag hanterar problemet. Vidare har studien resulterat i en modell för att säkerställa kontroll över informationsspridning när underhåll av säkerhetskritiska system outsourcas. Analysen har påvisat att det krävs ytterligare forskning inom området. Under arbetets gång har hänsyn tagits till vetenskapsrådets forskningsetiska principer.

1.2 Syfte

Syftet är att undersöka hur organisationer inom industrisektorn kontrollerar informationsspridning vid outsourcing av underhåll för säkerhetskritiska system. Studien ska presentera en strategi för att säkerställa kontroll vid outsourcing.

1.3 Forskningsfrågor

RQ 1: Vilka är de kritiska faktorerna för att behålla kontroll vid outsourcing av underhåll för säkerhetskritiska system?

RQ 2: Hur kan de identifierade kritiska faktorerna hanteras i verksamheten?

2. Metod

Avsnittet presenterar tillvägagångssättet för studiens skapandeprocess.

2.1 Angreppssätt

Forskningsdesignen för studien är en multipel fallstudie, då flera företag har studerats för att finna skillnader och likheter mellan dessa, vilket stärker reabiliteten (Yin, 2012). Internatbaserad sökning vad gäller etiska aspekter skapade medvetenhet och förståelse för etiska problem, vilket la grunden för en etiskt försvarbar studie (Lennerfors, 2019). Litteratursökning gjordes i tidigt skede för att identifiera forskningsgapet, vilket säkerställde studiens validitet (Patel & Davidson, 2003; Yin, 2009). Kurslitteratur och vetenskapliga artiklar gav kunskap och förståelse för området, vilket la grunden för studiens genomförande och problembakgrund (Blomkvist & Hallin, 2014). Problembakgrunden var avgörande för att skapa ett preliminärt syfte och frågeställningar (Blomkvist & Hallin, 2014). Studien är kvalitativ då resultatet baseras på intervjuer (Blomkvist & Hallin, 2014). Intervjuer som datainsamlingsmetod ger förståelse och kunskap gällande enskilda individers tankar, vilket skapar möjlighet att göra oanade upptäcker (Blomkvist & Hallin, 2014). Vidare valdes intervjuer för att skapa en allmän bild av problemet (Sohlberg & Sohlberg, 2013).

För att öka studiens generaliserbarhet och reliabilitet är litteraturinsamling avgörande då det specificerar samt förklarar det studerade området (Yin, 2012). Rapportens teoretiska referensram utgörs av sekundära källor i form av kurslitteratur och vetenskapliga artiklar (Blomkvist & Hallin, 2014). Högskolan i Gävles biblioteksdatabas har använts som verktyg för att finna kurslitteratur, vilket bidragit till kategorisering av litteratur utifrån ämnesområde som underlättat arbetet. Inläsning av teori skapade förståelse och kunskap kring området för att finna intressanta sökord till litteratursökningen (Patel & Davidson, 2003). Sökorden som valts är säkerhetskritiska system, management, hållbar utveckling, outsourcing, supply chain management, blockchain och Industri 4.0. Kurslitteratur baserat på sökorden har granskats i syfte att erhålla grundläggande fakta och bredda sökområdet. Vidare har informationen jämförts med vetenskapliga artiklar för att säkerställa dess reliabilitet (Blomkvist & Hallin, 2014). Insamlad teori har analyserats genom fördelning av data i separata kategorier i form av en tematisk analysmetod, vilket bidrog till att besvara studiens frågeställningar (Blomkvist & Hallin, 2014). Teoriavsnittet la grunden för att utveckla ett generaliserbart resultat när jämförelse skedde mot empiriskt

material (Yin, 2009). Jämförelsen hjälpte till att sortera bort litteratur som inte var betydelsefull för studiens analys och slutsats. Teoriavsnittet utvecklades noggrant för att kunna användas i analysen, då resultatet stärks av att det är flera forskare som stödjer samma teori (Yin, 2009). Trots att insamling av teori skedde före empiriinsamling anses arbetet ha en induktiv ansats, då intervjuernas resultat har jämförts med teori, i syfte att skapa förståelse för resultatet (Blomkvist & Hallin, 2014).

Beslutet att studera företag inom industrisektorn gjordes under problematiseringen. Genom internetbaserad sökning valdes företag utifrån samma bransch, vilka tillhör Sveriges största företag beräknat efter lönsamhet, där samtliga har digitaliserade och automatiserade processer. Samtliga respondenter har god kunskap inom området, vilket ansågs avgörande för att besvara intervjufrågorna. Trots studiens begränsade tidsram anses antalet intervjuade företag vara tillräckligt för studiens generaliserbarhet (Sohlberg & Sohlberg, 2013).

Inläsning på forskningsområdet gav förståelse för forskningsgapet samt möjliggjorde utformande av intervjufrågor där svaren syftade till att fylla gapet och säkerställa att nuvarande teori är tillämpbar i verkligheten (Patel & Davidson, 2003). Vidare bidrog det till studiens validitet (Yin, 2009). Intervjufrågorna bearbetades flera gånger för att säkerställa frågornas relevans utifrån syftet. Vidare togs två intervjuunderlag fram, i syfte att studera problemområdet ur olika perspektiv. Ett underlag anpassades för industriföretag som är i behov av underhåll samt ett till företag som utför underhåll.

För att komma i kontakt med ansvariga på respektive företag kontaktades företagens växel där namn, telefonnummer eller mailadress erhölls. Första kontakten med respondenterna skedde via telefon och mail. När företag nåddes via telefon gavs information om studiens syfte och medverkan tillfrågades. Vidare intervjuades tre företag via telefon och resterande erhöll ett mail med intervjuunderlaget. Företag där telefonkontakt inte var möjlig kontaktades via mail med information om studiens syfte där medverkan tillfrågades och intervjufrågor bifogades. Det var viktigt för studiens etiska aspekter att ge respondenterna tydlig information om studiens syfte och att tillfråga medverkan (Blomkvist & Hallin, 2014). Respondenterna erhöll en intervjuguide, vilken beskrev det studerade området, i syfte att ge respondenterna förståelse (Blomkvist & Hallin, 2014). Intervjuer som utfördes via telefon var semistrukturerade för att möjliggöra

öppna slutledningar och diskussion (Bryman, 2011). Telefonintervjuerna dokumenterades i Google docs under utförandet. Intervjuerna via mail innefattade frågor med en låg grad av strukturering och hög grad av standardisering då frågorna var formulerade med öppna svar (Patel & Davidson, 2003). Vidare besvarades frågorna i det bifogade underlaget. Samtliga intervjuer var konfidentiella då anonymisering var avgörande för att kunna genomföra intervjuerna (Patel & Davidson, 2003). Hänsyn har tagits till respondenter som inte haft möjlighet att besvara samtliga frågor, vilket är positivt för studiens reliabilitet (Yin, 2009).

Insamlade data har analyserats genom att skriva en sammanfattning utifrån varje enskild intervju. Valet att sammanställa intervjumaterialet i textform grundas i svarens omfattning och för att säkerställa förståelse för materialet samt finna samband mellan respektive intervju. Vidare har all data sammanställts i tabeller för att ge en överskådlig bild av resultatet. Detta har möjliggjort att komma fram till svarens bredd och är ett komplement till berättelser i textform. Resultatet har analyserats med en cross-case analys, vilket innebär skapandet av en tabell där en jämförelse sker mellan samtliga företag för att säkerställa validitet (Yin, 2009). Cross-case analysen bidrog till att identifiera kritiska faktorer när underhåll av säkerhetskritiska system outsourcas. Faktorerna analyserades för att finna tillvägagångssätt för att hantera dessa, vilket mynnade ut i en modell.

2.2 Metodreflektion

Studien fokuserar på industrisektorn och därmed kan inte ett liknande resultat garanteras om studien replikeras på en annan bransch. Det studerade området tros vara mer kritiskt för statlig verksamhet, därför kan framtida studier inkludera denna bransch, i syfte att identifiera kritiska faktorer. För framtida forskning kan området studeras i större omfattning för att säkerställa generaliserbarhet. Studiens forskningsmetodik kan möjligtvis ha påverkat resultatet då intervjuerna utförts på olika sätt, vilket kan påverka studiens reliabilitet. Genom att utföra intervjuer på samma sätt säkerställs att respondenterna får samma möjlighet att förmedla tankar och idéer, vilket varit begränsat i intervjuerna via mail. Intervjumetoderna anses separat vara två tillförlitliga tillvägagångssätt, däremot kan viss kritik riktas till att kombinera metoderna (Blomkvist & Hallin, 2014; Yin, 2009). Däremot anses valet att kombinera metoderna vara viktigt för studiens slutsats och tidsram då det bidrog till större svarsfrekvens inom kort tid (Yin,

2009). I syfte att öka kunskap och förbättra generaliserbarhet kan studiens kompletteras med en enkätundersökning, för att öka antalet respondenter och företag (Blomkvist & Hallin, 2014).

Validitet har säkerställts genom att samtliga avsnitt kontinuerligt jämförts med syftet och frågeställningarna. Vidare har ett stort antal källor samt stöd från handledare stärks studiens validitet (Yin, 2009). För att stärka studiens validitet kan en replikering av studien vara aktuellt (Yin, 2009). För att säkerställa reliabilitet har fokus varit att jämföra resultatet mot teoriavsnittet. Däremot hade jämförelse med syfte och frågeställningar i större utsträckning kunnat stärka studiens reliabilitet (Yin, 2009). Flera respondenter har påpekat att intervjuguiden saknade en tydlig definition av ett säkerhetskritiskt system. Detta kan ha påverkat studiens resultat i form av att respondenterna inte hade tillräcklig kunskap för att besvara frågorna. En tydlig definition av vad säkerhetskritiska system innebär tros bidra till mer utförliga svar på intervjufrågorna. Studien anses vara etisk försvarbar då hänsyn tagits till vetenskapsrådets forskningsetiska principer inom humanistisk-samhällsvetenskaplig forskning (Blomkvist & Hallin, 2014; Patel & Davidson, 2003). Vidare är det av stor vikt att hänsyn tas till etiska aspekter då arbetet ska offentliggöras samt för Högskolan i Gävles bidrag till social- och ekonomisk hållbarhet.

3. Teoretisk referensram

Avsnittet presenterar studiens insamlade litteratur.

3.1 Outsourcing

Outsourcing innebär att en organisations aktiviteter utförs av ett externt företag (Durst & Edvardsson, 2014). Strategin syftar till att skapa relationer med externa partners som kan utföra delar av verksamheten enligt företagets förväntningar och krav (Mishra et al., 2017), till lägre kostnad, högre kvalitet, leveransprecision och tillförlitlighet (Edgren & Skärvad, 2014). Outsourcing av aktiviteter bidrar till skapandet av nätverk som består av flera företag, vilka tillsammans skapar en enhet på marknaden. Företagen i nätverket är ansvariga för en varsin del i värdekedjan, som dessa är specialiserade på. Drivkrafter att skapa ett nätverk är utveckling av informations- och kommunikationsteknik, globalisering samt snabba förändringar på marknaden (Edgren & Skärvad, 2014). Kommunikationsteknik möjliggör för parterna i nätverket att kommunicera i realtid, där dessa alltid är uppkopplade mot varandra. Detta möjliggör att aktiviteter samordnas och synkroniseras, vilket ökar nätverkets konkurrenskraft (Edgren & Skärvad, 2014).

En orsak till outsourcing är att sänka företagets kostnader genom minskad intern arbetskraft, då det är kostsamt med expertkompetens (Murthy et al., 2015). Outsourcing bidrar till att företag kan fokusera på kärnverksamheten, vilket skapar konkurrensfördelar (Edgren & Skärvad, 2014; Murthy et al., 2015). Företag kan med fördel outsourca säkerhet, eftersom det innebär att data lagras på flera ställen samtidigt (Carlsson & Jacobsson, 2012). Nackdelar med outsourcing är ökad beroendeställning till leverantörer samt högre samordnings- och kommunikationskostnad (Edgren & Skärvad, 2014). Beslut om outsourcing ska därför grundas i ställningstagande vad gäller affärsmål, timing, outsourcingsalternativ, lämpliga aktiviteter att outsourca, val av leverantör, potentiella risker samt vilka system som behövs för en effektiv övervakning (Murthy et al., 2015).

3.1.1 Underhåll

Betydelsen av underhåll varierar mellan företag (Hagberg & Henriksson, 2018) och är en kritisk funktion som syftar till att bevara eller återställa utrustning i ett användbart tillstånd (Van Niekerk & Visser, 2010). Underhållsaktiviteter innefattar korrigering av buggar, uppgraderingar, anpassning av system till nya krav och förbättrad prestanda (Flodén, 2013). Vidare är underhåll en ständigt pågående process som krävs under hela

objektets livstid, i syfte att upprätthålla funktionalitet. För att minska uppkomsten av avvikelser kan underhåll ske både passivt som aktivt, vilket innebär att problem åtgärdas vid uppkomst eller att system ständigt kontrolleras (Flodén, 2013). Underhållsaktiviteter är nödvändiga för att uppnå konkurrenskraft, då det påverkar säkerhet, miljö och ett företags totala ekonomi (Hagberg & Henriksson, 2018).

För att uppnå hög kvalitet i underhållsarbete krävs fokus på flera faktorer, vilka är; delaktighet bland medarbetare, engagerat ledarskap, faktabaserat beslutsfattande, kompetensutveckling, kundorientering, kvalitetssäkrande åtgärder, långsiktighet, att lära av andra företag, processorientering, samhällsansvar, samverkan, snabba reaktioner (Hagberg & Henriksson, 2018) och ständig förbättring (Hagberg & Henriksson, 2018; Van Niekerk & Visser, 2010). För att uppnå underhåll i världsklass krävs målsättning vad gäller underhållets önskade resultat, kartläggning av nuläge samt att företaget utvecklar en metod för att uppnå målet. Underhållsarbetet kräver processorientering, involvering av samtliga medarbetare, kontinuerlig utvärdering (Hagberg & Henriksson, 2018), god planering och proaktivitet (Van Niekerk & Visser, 2010).

Underhåll innebär främst att minska kostnader på kort sikt, istället för att maximera värdet genom långsiktiga mål och kontinuerlig förbättring (Murthy et al., 2015). Ledningens engagemang och kompetens är avgörande för att uppnå målsättning vad gäller underhåll (Hagberg & Henriksson, 2018). Underhåll kräver medarbetare som besitter kompetens (Hagberg & Henriksson, 2018; Van Niekerk & Visser, 2010), vilket innebär ständig kompetensutveckling för medarbetare, ledare och andra partners inom underhållsverksamheten. Medarbetarnas kunskap och förståelse för underhållets ekonomiska betydelse är avgörande för underhållsarbetet, då det skapar engagemang för ständig förbättring. Ett helhetsperspektiv är avgörande för att utveckla underhållsarbetet, vilket kräver resurser i form av konsulter med expertkompetens, involvering av leverantörer, centrala underhållsexperter för hela företaget, avdelningens egna underhållsexperter samt medarbetare. Vidare bör underhållet vara integrerat mellan avdelningar och underhåll, såväl extern som internt (Hagberg & Henriksson, 2018). Ny teknik möjliggör analysering och bearbetning av data i realtid, där underhållsinformation med fördel kan samlas i ett underhållssystem, både när underhåll sker externt och internt. Däremot kräver ett underhållssystem säkerhet då ny teknik, såsom Internet of Things medför säkerhetsrisker (Hagberg & Henriksson, 2018).

3.1.2 Outsourcing av underhåll

Det är vanligt att företag outsourcar hela eller delar av underhållet, då outsourcing anses bidra till ökad kunskap i verksamheten (Ali-Marttila et al., 2017; Hagberg & Henriksson, 2018; Murthy et al., 2015). Orsaker att outsourca underhåll kan vara att företag inte lyckas utveckla underhållet likt nödvändigt eller önskat, höga kostnader samt att underhållet inte tillhör kärnverksamheten (Hagberg & Henriksson, 2018). Outsourcing är en strategi som skapar värde för både kunden och leverantören, då det bidrar till en effektiv hantering av underhåll. Beslut att outsourca underhåll bör vara strategiskt korrekt, vilket innebär att vald leverantör besitter lämplig kompetens (Van Niekerk & Visser, 2010). Vid outsourcing är även ett leverantörsavtal viktigt, då det fastställer kostnad, leverantörens ansvar, vilka krav som ställs från kunden samt tillgänglighet i form av drifttimmar och utryckningstid vid akuta problem. Viktiga faktorer att beakta vid outsourcing av underhåll är; intern kompetens, klargöra vilka arbetsuppgifter som ingår i underhållet, leverantörens medverkan i möten som berör underhåll, administration och feedback, leverantörens effektiviseringsmål, hur önskad utveckling ska säkerställas samt hur tillgångar ska ägas och utvecklas (Hagberg & Henriksson, 2018). Ett bra outsourcat underhåll är när relationen bidrar till värde för båda parterna, när outsourcingen är långsiktigt hållbar samt bidrar till god prestanda och möjliggör för kontinuerlig förbättring (Van Niekerk & Visser, 2010).

3.1.3 Leverantörsrelationer

Relationer till leverantörer kräver tillit och säkerhet, där samtliga parter delar kompetens och värderingar. Hög grad av tillit innebär att företag vågar uttrycka idéer och åsikter. Vidare är öppen kommunikation och ärlighet viktigt, där initiativ tas utan rädsla för misslyckande. När tillit brister i ett partnerskap undanhålls exempelvis delar av information. Hög tillit kan leda till att parterna inte ifrågasätter varandras beslut i tillräcklig utsträckning (Christopher, 2016). Traditionella leverantörsrelationer kan hållas på en armlängds avstånd med korttidskontrakt, vilket ofta grundas i prispressning och konkurrenskraft. Långsiktiga partnerskap innebär ett nära samarbete, i syfte att samverka på många nivåer. Företagen i ett långsiktigt partnerskap bidrar till varandras utveckling och förbättring (Edgren & Skärvad, 2014). Tillit är avgörande vid partnerskap och enkla kundrelationer måste förvandlas till trovärdiga affärsrelationer, vilket kan upplevas svårt på grund av anonymitet (Jansen, 2017).

3.2 Säkerhet

Industri 4.0 och Internet of Things tillför ny teknologi till företag, däremot ökar säkerhetsrisker kraftigt, exempelvis genom ekonomisk påverkan, då intrång i system kan slå ut delar av verksamheten under lång tid. Säkerhetsfaktorer att fokusera på när marknaden förändras mot ökad digitalisering och automatisering är obehörigt intrång som orsakar oönskad informationsspridning utanför nätverket. Vidare är det av stor vikt att medarbetare är medvetna och har kunskap om säkerhetsrisker, för att minimera hotbilden (Pereira et al., 2017). Ständigt växande datavolymer, krav på ökad mobilitet, samverkan och delning av information med externa parter kräver ökad säkerhet samt skydd av data. Företag möter utmaningar vad gäller säkerhet, då ökad integrering kräver hög säkerhet (Vaidya et al., 2018). Vidare bör företag skydda data mot obehörigt intrång (Oesterreich & Teuteberg, 2016).

Säkerhet handlar om skydd av tillgångar, vilket innebär att det är avgörande att känna till företagets tillgångar och dess värde (Gollmann, 2011). Säkerhetssystem kräver auktoriserade tillstånd där obehöriga ej har tillträde. Vanligtvis innehåller säkerhetssystem gränssnitt som möjliggör att konfigurera system och rapportera specifika händelser eller övervaka åtkomst (Bishop, 2004). Det är viktigt att företag implementerar säkerhetssystem i lämplig nivå för att undvika hot gällande ekonomisk, nationell och publik säkerhet. Företag måste förstå riskbilden, skapa medvetenhet i organisationen och stå upp för nödvändiga säkerhetskontroller. Säkerhetssystem måste beakta såväl teknik som organisatoriska och humana faktorer (Jansen, 2017).

Skapandet av nätverk innebär ökad integrering mellan system, vilket bidrar till komplexa förhållanden i säkerhetssystemet. Säkerhet måste bevaras vid ökad integrering och kommunikation mellan enheter (Jansen, 2017). Ett alternativ för att bevara säkerhet är outsourcing, då det minskar kostnader eftersom säkerhetsföretag kan tillhandahålla kvalificerad IT-säkerhet och kompetens (Jansen, 2017). Däremot finns det en ökad risk för informationsspridning när företag outsourcar då leverantören och kunden bedömer informationens känslighet olika (Heickerö, 2012). Vidare blir det allt vanligare att företag outsourcar lagring och underhåll av information i molntjänster hos ett säkerhetsbolag, vilket sänker kostnader då företaget inte behöver investera i system. Detta bidrar till säkerhetsbrister då förmågan att ständigt kontrollera uppfyllelse av kundkrav är svårt (Heickerö, 2012).

3.2.1 Informationssäkerhet

Informationssäkerhet handlar om att säkerställa sekretess, integritet och tillgång till information, i syfte att skydda information (Hallberg, Johansson, Karlsson, Lundberg, Lundgren & Törner, 2017; Wangen, Snekkenes & Hallstensen, 2017). Informationssäkerhet är en tolkningsfråga, vilket grundas i organisationens kultur som påverkar hur säkerhet hanteras. Informationshantering förändras snabbt och påverkas av faktorer såsom virtualisering, molnbaserade nätverk och informationsteknologi (Hallberg et al., 2017). Vid implementering av molnbaserade system är många företag oroliga för säkerheten vad gäller obehörig åtkomst till system och ökad risk för informationsspridning (Carlsson & Jacobsson, 2012). Vidare medför krav på lättillgänglig information en utmaning för informationssäkerheten, då snabba förändringar på marknaden gör det svårt att förutsäga framtida utveckling. Trots investering i säkerhetssystem tycks brister i informationssäkerhet öka, vilket beror på medarbetarnas bristande kompetens avseende informationssäkerhet och kan leda till säkerhetsincidenter (Hallberg et al., 2017).

Informationssäkerhet grundas i såväl sekretess som riktighet och tillgänglighet. Detta innebär att information endast är tillgänglig för behöriga och att förändrad information kontrolleras (Hallberg et al., 2017). Informationssystem definieras som integrering mellan individer, utrustning och procedurer, som tillsammans samlar in, lagrar och hanterar data (Flodén, 2013). Det är av stor vikt att systemen är etablerade och underhålls regelbundet (Van Niekerk & Visser, 2010), vilket gör information tillgänglig för planering, implementering och kontroll (Flodén, 2013). Informationssystem är viktiga för att säkerställa framgångsrik hantering av outsourcingavtal (Van Niekerk & Visser, 2010). Blockchain är ett informationsverktyg som säkrar transaktioner mellan parter i ett affärsavtal. Vidare är blockchain kritiskt och bygger på tillit mellan parter, därför är det avgörande att det finns säkerhet i systemet. Säkerhet skapas genom att parterna har privata koder till transaktionen tills dess att koden är ogiltig. Blockchain säkerställer en hög nivå av säkerhet som innebär att obehöriga inte kan få tillgång till information (Skinner, 2016).

Säkerhet i leverantörskedjan har blivit en stor utmaning på grund av integration och samverkan mellan parter i nätverket (Yeboah-Ofori & Islam, 2019). Snabb tillväxt av antalet molnbaserade system och allt fler tillämpningar leder till förhöjd hotbild (Ashibani & Mahmoud, 2017; Zegzhda, Vasil'ev & Poltavtseva, 2018). Hot förekommer för alla

enheter som kommunicerar via internet, där målobjekt är stater, enskilda företag och individer (Bendovschi, 2015; Heickerö, 2012). Avsikten med obehörigt intrång är exempelvis att erhålla information och data som företaget skyddar (Heickerö, 2012). Obehörigt intrång leder till förlorad information och inkomst samt störningar i verksamheten. Orsaker till säkerhetsbrott är mänsklig faktor, systems sårbarhet och avsiktliga attacker. När ett intrång sker beror det delvis på verksamhetens sårbarhet vad gäller informationssäkerhet (Bendovschi, 2015). Enligt Heickerö (2012) är det viktigt att det finns ett system för kommunikation i realtid när samhällets utveckling går mot högteknologi, vilket kräver integrerade system. Vidare medför det snabb spridning av avvikelser i systems sammankopplade enheter, vilket ställer krav på förmågan att skydda och säkra samtliga led i värdekedjan (Heickerö, 2012). För att säkra kontroll måste företag utvärdera säkerheten i realtid (Boiko, Shendryk & Boiko, 2018). Förtroendet för att lagra och producera känslig information i datorsystem har ökat, vilket innebär att dessa system lättare blir angripna. Att endast säkra nätverket är inte en tillräcklig lösning för ett erhålla kontroll (Kaur & Sharma, 2017).

3.2.2 Säkerhet vid extern åtkomst

Informationssäkerhet upprätthålls genom att begränsa utomståendes åtkomst till informationssystem. Organisationen skall med utomstående part som ges behörighet till information och data göra en överenskommelse som definierar ansvarsfördelning och eventuella åtgärder i ett avtal (Bowin, 2004). Vid involvering av en extern part bör ett sekretessavtal övervägas för att reglera säkerhetsvillkor. Vid outsourcing bör risker, rutiner och åtgärder i fråga om säkerhet för informationssystem beaktas i avtalet, vilket är betydande vid bibehållande av säkerhetsnivån. Vidare bör ett flertal faktorer beaktas, såsom sekretess, åtkomst, informationsspridning, hantering av material samt säkerhetsklassificering i avtalet. Vid outsourcing överlåts vanligtvis ansvaret för informationssäkerheten på utomstående part (Bowin, 2004).

3.2.3 Säkerhetspolicy

En informationssäkerhetspolicy är ett verktyg som anger en tydlig riktning för arbetet med informationssäkerhet och ska förankras i verksamheten. Organisationer som besitter kritisk information kan med fördel implementera en informationssäkerhetspolicy (Bowin, 2004). En informationssäkerhetspolicy ska besvara vad som ska skyddas, vem som är ansvarig, hur arbetet ska bedrivas, hur incidenter skall hanteras samt vad påföljden blir

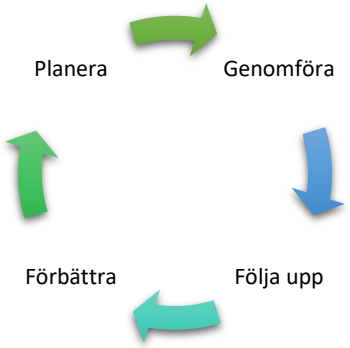
om policyn inte efterlevs. Policyn ska vara kommunicerbar, relevant i förhållande till verksamheten, långsiktig, övergripande och visa riktning (Bowin, 2004). Leverantörer, entreprenörer, kunder och samarbetspartners skall informeras om organisationens informationssäkerhetspolicy, syn på säkerhet samt vilka önskemål och krav som är förknippade med policyn. Nyckelfaktorer som bör ingå i policyn är definitionen av informationssäkerhet, säkerhetskrav, övergripande- och detaljmål, ansvarsfördelning samt en beskrivning av uppföljningssystemet (Bowin, 2004). När ett företag implementerar en informationssäkerhetspolicy är det viktigt att utföra en riskbedömning, i syfte att bedöma hotbild och verksamhetens sårbarhet. Skydd av information och data kräver resurser och är grunden för en väl utformad säkerhetspolicy (Flowerday & Tuyikeze, 2016).

3.2.4 Standard för informationssäkerhet

ISO 27001:2017 är en kravstandard som syftar till att upprätta, införa, underhålla samt ständigt förbättra ett ledningssystem för informationssäkerhet, vilket kan användas både internt och externt. Ledningssystem för informationssäkerhet bidrar till att bedöma organisationens förmåga att uppfylla informationssäkerhetskrav, då den innefattar krav på bedömning och behandling av informationssäkerhetsrisker (Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav (Swedish Standards Institute, 2017)). Implementering av ett ledningssystem för informationssäkerhet är ett strategiskt beslut för en organisation. ISO 27001:2017 bevarar konfidentiell information, riktighet och tillgänglighet genom tillämpning av en riskhanteringsprocess, vilket ger förtroende till berörda parter. Det är av stor vikt att ledningssystemet är en integrerad del av organisationens processer, där hänsyn tas till informationssäkerhet vid utformning av processer, informationssystem och säkerhetsåtgärder (Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav (Swedish Standards Institute, 2017)). ISO 27001:2017 bidrar till att styra och kontrollera informationstillgångar, i syfte att säkerställa kontinuitet, vilket kräver spetskompetens inom ett eller flera områden. Nätverk möjliggör informationsdelning i realtid vad gäller hot, hantering av hot, råd samt kompetens. Det är viktigt att organisationer begränsar informationsutbytet så att konfidentiell information inte delges obehöriga (Bowin, 2004). Ökat antal aktiviteter i informationssystem vid outsourcing kräver etablerade riktlinjer för att upptäcka hot i tidigt skede (Kaur & Sharman, 2017).

3.2.4.1 PDSA-Cykeln

PDSA-cykeln innefattar grundläggande komponenter för en organisations strategiska arbete och inkluderar planering, genomförande, analysering och uppföljning samt förbättring. Vidare innebär detta att organisationen ska analysera dagsläget och upprätta mål att arbeta mot. Det är även viktigt att måluppfyllelse utvärderas samt att åtgärder upprättas vid brister. Vanligtvis tillämpas modellen för ledningssystem men används även vid enskilda fall. Arbetet skall ske i kontinuerliga cykler för att säkerställa ständig förbättring (Ammenberg, 2012).



Figur 1: Figuren illustrerar stegen i PDSA-cykeln.

4. Resultat

Nedan presenteras elva stora företag inom industrisektorn, vilka utgör studiens resultat. Industrisektorn har valts för att branschen påverkas starkt av snabba förändringar på marknaden samt att processer ständigt utvecklas mot ökad automatisering och digitalisering. Vidare innebär denna utveckling en ökad risk för informationsspridning (Pereira et al., 2017). Studiens företag består av underhållsleverantörer, vilka underhåller säkerhetskritiska system samt tillverkande företag, vilka har säkerhetskritiska system som kräver underhåll.

Tabell 1: Tabellen illustrerar en sammanfattning av det resultat som framkommit av intervjuer.

Företag	**Affärsområde**	**Respondent**	**Outsourcar Ja/Nej**	**Påverkande faktorer**
Företag 1	Underhållsleverantör	VD	N/A	N/A
Företag 2	Underhållsleverantör	Project Manager	N/A	N/A
Företag 3	Underhållsleverantör	Underhållsutvecklare	N/A	N/A
Företag 4	Tillverkande företag	Senior Business Analyst	Nej	Resurser & kontroll
Företag 5	Tillverkande företag	General Manager Corporate	Nej	Kompetens
Företag 6	Tillverkande företag	Underhållschef	Nej	Kompetens & kontroll
Företag 7	Tillverkande företag	Project & Production Development Manager	Nej	Kontroll
Företag 8	Tillverkande företag	Underhållschef	Ja	Kostnadseffektivitet
Företag 9	Tillverkande företag	Sektionschef FU	Ja/Nej	Kostnadseffektivitet, kompetens & leveransfrågor
Företag 10	Tillverkande företag	Underhållschef	Ja	Kompetens
Företag 11	Tillverkande företag	PLM Arkitekt	Ja	Resurser, kompetens, kostnader, legala krav & samverkan

4.1 Underhållsleverantör

Nedan presenteras material som framkommit under intervjuer med underhållsleverantörer.

Företag 1 är en underhållsleverantör med ca 50 kunder. Relationen till kunder påverkas av att det är underhåll av säkerhetskritiska system som utförs, i form av kritiskt beslutsfattande och nära samarbete. Det är viktigt med en god kundkännedom och att företaget har förståelse för kundens verksamhet samt systemens innebörd, verksamheten måste ses i dess helhet. En problematisk faktor som identifierats i relationen mellan parterna är kundens upplevelse av förlorad kontroll, vilket innebär att relationen måste bygga på trygghet och tillit. Företaget ansvarar för hela och delar av underhållet för säkerhetskritiska system, vilket bland annat påverkas av kundens mognad då nystartade företag har mindre benägenhet att outsourca hela underhållet. Vidare sker underhåll av kundens system dygnet runt. För att säkerställa uppfyllelse av kundkrav upprätthålls nära kontakt med kunder, vilket anses avgörande för en lyckad outsourcing. Enligt respondenten är informationsspridning ingen risk eftersom arbetet sker enligt krav. Outsourcing kräver ett väl genomtänkt avtal och vid en eventuell informationsspridning bär underhållsleverantören ansvaret, då avtalet reglerar dessa avvikelser.

Företag 2 är en underhållsleverantör med ca 1000 kunder. Relationen till kunder påverkas av att det är underhåll för säkerhetskritiska system som utförs i form av undanhållen information med orsak av säkerhetsklassad information och data. Vidare kräver en kundrelation ett tydligt avtal som innefattar omfattning och förväntningar parterna emellan. Ett nära samarbete och en god personkemi är viktigt i relationen till kunder. Vad gäller problematiska faktorer i relationen är dessa få, och vid problem upprättas rutiner för att säkerställa personsäkerhet och verksamhetens fortlöpande. Företaget ställer höga krav på utförande, vilket säkerställer att kundkrav uppfylls. Vidare tillhandahålls certifierade serviceingenjörer inom IT-säkerhet och företaget är ständigt uppdaterade vad gäller branschstandarder för IT-säkerhet. Företaget anser att outsourcing av underhåll för säkerhetskritiska system inte medför en ökad risk för informationsspridning. Vidare finns utarbetade rutiner för tekniska delar och kompetens, i syfte att hantera oönskad informationsspridning. Merparten av underhåll baseras på företagets allmänna leveransbestämmelser, däremot tillhandahåller ibland kunden ett eget avtal. Företaget bär aldrig ansvar vid oönskad informationsspridning.

Företag 3 är underhållsleverantör till ca fyra kunder. Relationen mellan leverantör och kund ska vara av god kvalitet, vilket inkluderar trygghet. Vidare påverkas inte relationen av att det är underhåll för säkerhetskritiska system som outsourcas. Vid underhåll av säkerhetskritiska system anses det vara viktigt med ökad säkerhet för att minska risk för informationsspridning. Underhåll sker för hela och delar av system, vilket sker kontinuerligt, planerat samt vid akuta åtgärder. Företaget säkerställer att kundkrav uppfylls genom formella beställningar och samordning gällande säkerhet för medarbetare, maskiner samt system. Det finns en ökad risk för informationsspridning när underhåll av säkerhetskritiska system outsourcas och för att kontrollera situationen är det viktigt att det finns förtroende till serviceteknikerna samt att ett sekretessavtal upprättas.

4.2 Tillverkande företag

Nedan presenteras material som framkommit under intervjuer med tillverkande företag.

Företag 4 har säkerhetskritiska system i form av ERP system, vilket innefattar produktionsplanering, produktionsuppföljning, recepthantering, kvalitetssystem samt frisläppande av produkter. Vidare kräver systemen underhåll i form av fortlöpande ”patchningar” och ”enhancements”. Företaget har tidigare outsourcat underhåll av säkerhetskritiska system, numera sker underhåll internt. Valet att utföra underhåll inom företaget grundas i säkerställande av nödvändiga resurser och att inte behöva förlita sig på externa aktörer. Vidare upplever företaget ökad kontroll av systemförvaltning och dataintegritet när underhåll utförs internt. I dagsläget finns inga nackdelar att utföra underhåll av säkerhetskritiska system internt, däremot finns svårigheter att anpassa resurser till ett fluktuerande behov.

Företag 5 har säkerhetskritiska system såsom CAD/PLM system, affärssystem och e-commerce system. Samtliga system kräver underhåll, vilket företaget utför internt. Företaget har däremot stödfunktioner som externa konsulter utför vid behov. Valet att inte outsourca underhåll av säkerhetskritiska system beror på att företaget har ett fungerande arbetssätt för underhåll. Underhåll är en viktig kompetens att besitta internt, därav anses inte outsourcing av hela underhållet vara ett alternativ. Det finns inga nackdelar med att utföra underhåll internt, däremot kan outsourcing vara ett framtida alternativ om behov uppstår.

Företag 6 har säkerhetskritiska system i form av processtyrningssystem, informationssystem, säkerhetssystem för processutrustning och underhållssystem. Systemen kräver kontinuerligt underhåll i form av komponentbyten, programmering och uppdatering. Underhållet sker internt, då företaget vill kontrollera underhållsaktiviteter samt behålla och utveckla intern kunskap. En nackdel med att utföra underhåll internt är att underhållet kräver expertkompetens, vilket kan vara svårt att underhålla.

Företag 7 har ett säkerhetskritiskt affärssystem som kräver underhåll. Underhållet outsourcas inte då företaget vill kontrollera data och information i affärssystemet. Vidare anser företaget att det inte finns någon nackdel att utföra underhåll internt.

Företag 8 har system, vilka är säkerhetskritiska på grund av inloggningskoder. Systemen kräver underhåll, främst vad gäller IT, vilket outsourcas. Underhållsleverantören ansvarar för hela underhållet och vid avvikelser tillkallas en jour. Outsourcing av underhåll utförs med orsak av kostnadsfördelar. Underhållsleverantören är internationell, vilket innebär att språket kan leda till missförstånd. Vidare hålls relationen till leverantören på en armlängds avstånd. Leverantörsrelationen påverkas av det säkerhetskritiska systemet. Företaget anser att en leverantörsrelation kräver god kommunikation och snabb respons på förändringar. För att säkerställa att leverantören uppfyller krav som ställs sker utvärdering med symboler efter varje enskilt fall. Avtalet säkerställer att den part som sprider oönskad information bär ansvaret.

Företag 9 har flera säkerhetskritiska system, exempelvis eldistribution till transformatorer och drivsystem, vilket styr maskiner. Systemen kräver underhåll i form av uppdateringar och uppgraderingar för att motsvara företagets behov. Vidare utförs underhåll både internt och outsourcas. Uppdateringar utförs av systemleverantören, medan övrigt underhåll sker från central IT-avdelning, vilka hanterar olika typer av uppdateringar. Företaget arbetar med systemens optimeringar och förändringar på daglig basis. Underhåll utförs delvis internt då det bidrar till kostnadseffektivitet, däremot anser respondenten att det finns nackdelar att utföra underhåll internt då expertkompetens begränsas. Detta innebär att företaget besitter en bred grundläggande kompetensbas. Expertkompetens tas in externt vid avvikelser, uppdatering eller större förändringar i systemen. Outsourcing av underhåll för vissa aktiviteter baseras på kostnads- och

leveransfrågor. Relationen till underhållsleverantören påverkas inte av att det är ett säkerhetskritiskt system som underhålls, då samtliga avtal har premisser kring förväntningar. Respondenten anser däremot att tillväxten av molntjänster kan komma att förändra situationen. Företaget strävar efter ett nära samarbete med leverantören och undviker att vara beroende av leverantören på grund av kostnader. En problematisk faktor som identifierats i relationen till underhållsleverantören är konkurrensförhållanden till företag som anlitar samma leverantör. Vid molntjänster och internetbaserade system är det viktigt att leverantören är medveten om risker. Företaget säkerställer att leverantören uppfyller krav genom målsättningar, uppföljning och en öppen dialog. När underhåll outsourcas har inte företaget kontroll över informationsspridning. Informationsspridning anses inte vara en kritisk faktor i jämförelse med IT-branschen och säkerhetskritiska system anses inte påverka. Kontroll över processerna när underhåll av säkerhetskritiska system outsourcas bevaras genom att alltid vara styrande i relationen till leverantören.

Företag 10 har två säkerhetskritiska system, ABB AC450 och Level 2: Prins, vilka är säkerhetskritiska då all information och data finns sparade i systemen. Båda systemen kräver underhåll i form av uppdateringar och förbättringar. En stor del av företagets systemunderhåll outsourcas, där underhåll sker vid avvikelser. Valet att outsourca grundas i kravet på expertkompetens, vilket är svårt att utveckla och upprätthålla. Relationen till underhållsleverantören påverkas av att det är ett säkerhetskritiskt system som outsourcas i form av strängare krav, en omfattande bakgrundskoll samt ett nära samarbete. Problematiska faktorer i relationen till leverantören är förmågan att upprätthålla servicegraden. Leverantörsrelationen kräver struktur, beskrivning av tillvägagångssätt, vilka parametrar som påverkas samt att det sker en provkörning efter förändringar i systemet. Det är svårt att kontrollera om leverantören uppfyller ställda krav då det kräver insyn och kompetens. Vad gäller informationsspridning anses det vara en kritisk faktor i verksamheten samt att risken ökar när underhållet outsourcas. Vidare har företaget begränsad kontroll avseende informationsspridning, däremot kontrolleras processer genom att företaget äger programmet och koder. Informationsspridning kontrolleras genom ett reglerat avtal med leverantören utifrån parternas överenskommelse.

Företag 11 har säkerhetskritiska system i form av PLM, ERP, CRM och MES-systems, vilka samtliga kräver underhåll. Företaget outsourcar underhåll för samtliga komponenter i systemen. Underhållet kräver flera företags involvering och det förekommer att komponenter underhålls av interna IT-resurser. Leverantören underhåller fyra olika områden, människor, processer, verktyg och data. Vidare inkluderar underhållet funktioner såsom systemövervakning både kontinuerligt och periodiskt, resurshantering för att optimera systemen samt stöd och ständiga förbättringar. Företaget har valt att outsourca på grund av resurstillgång, expertkompetens, kostnadsfördelar, legala krav, samverkan mellan områden och relationer. Relationen till leverantören påverkas av att det är underhåll av ett säkerhetskritiskt system som outsourcas, då underhållsavtalet kräver en större omfattning och är väl genomtänkt. Vidare krävs förtydligande och dokumentation för affärsmässiga IT-processer som stödjer specifika aspekter vid snabba och normala förändringar. Problem i leverantörsrelationen är omedvetenhet om leverantörens ansträngning av lösa problem samt att information som delges kan vara bristfällig. Vidare är kultur en problematisk faktor till att lösa problem då slutanvändarna av system är mer hängivna att lösa problem snabbt än de medarbetare som inte är i kontakt med systemet.

Relationen till underhållsleverantören kräver tillit, proaktivitet, innovation, ständig förbättring, uttalat ägarskap av data, personspecifika licenser och tystnadsplikt. Inkludering av samtligt delar upplevs däremot svårt i en leverantörsrelation. För att säkerställa att leverantören uppfyller krav skapas ett team som har moral och tillit åt båda hållen samt att leverantörer utvärderas årligen. Informationsspridning är en kritisk faktor och företaget anser att digitalisering ökar risken. Outsourcing av underhåll för säkerhetskritiska system ökar risken för informationsspridning, däremot är kontraktet till leverantörer vanligtvis snävare än interna kontrakt mellan företagets olika avdelningar. Risken att förlora kritiskt data anses vara större när underhållet sker internt jämförelsevis med outsourcing, däremot är det sällan helt förstått av inblandade parter. Företaget har kontroll över informationsspridning, speciellt vad gäller kritiska och känsliga data. För att bevara kontroll är vanligtvis outsourcing fördelaktigt, då leverantören bidrar till att hitta information som behövs i processer eller att hitta detaljer i processen. Ett detaljerat sekretessavtal mellan företaget och underhållsleverantören beskriver vem som bär ansvaret över och äger data samt vem som äger systemet samt data i det, ibland inkluderas även processägare.

5. Analys

För att undersöka problemområdet har intervjuer med elva stora företag inom industrisektorn utförts i syfte att identifierat respondenternas syn på problemområdet. Studien har identifierat flera faktorer som är viktiga att ta hänsyn till för att kontrollera informationsspridning vid outsourcing av underhåll för säkerhetskritiska system. Faktorer som identifierats är kompetens, kontroll, nära samarbete, tillit, god kommunikation, kundkrav samt god kännedom om verksamheten. För att hantera faktorerna och stärka företags säkerhet föreslås en modell som bygger på flera komponenter, vilka tillsammans bidrar till ökad kontroll av informationsspridning.

5.1 Underhållsleverantörer

Tabell 2: Tabellen visualiserar en cross-case analys av resultatet från underhållsleverantörerna.

Företag	**1**	**2**	**3**
Antalet kunder	Ca. 50	Ca. 1000	Ca. 4
Påverkas kundrelationen av att det är ett säkerhetskritiskt system?	Ja	Ja	Nej
På vilket sätt?	Kritiska beslut, nära samarbete	Undanhållen information pga. säkerhetsklassad information och data	N/A
Vad är viktigt i en kundrelation?	God kundkännedom, förståelse för verksamheten och systemets innebörd	Tydligt avtal, nära samarbete, god personkemi	God kvalitet, trygghet
Finns det några problem i relationen?	Kunden upplever förlorad kontroll	Få problem, rutiner upprättas för att säkerställa personsäkerhet & verksamhetens fortlöpande	Nej
Sker underhåll för delar av eller hela system?	Hela & delar	Hela & delar	Hela & delar
När utförs underhåll?	Hela tiden	Ej angivet	Hela tiden & vid behov
Hur säkerställs att krav uppfylls?	Nära kontakt med kunden	Högre krav än kunder, certifierade serviceingenjörer, branschstandarder för IT-säkerhet	Formella beställningar, offerter, samordning
Finns en ökad risk för informationsspridning?	Nej	Nej	Ja
Arbetssätt för att bevara kontroll över informationsspridning?	Finns ej, behövs inte	Rutiner för tekniska delar, kompetens	Sekretessavtal, tillit till servicetekniker
Hur ser avtalet ut? Ansvar vid informationsspridning?	Underhållsleverantören bär ansvaret, regleras i avtal	Avtalet baseras på allmänna bestämmelser, underhållsleverantören bär inte ansvaret	Ej angivet

5.1.1 Vilka är de kritiska faktorerna för att behålla kontroll vid outsourcing av underhåll för säkerhetskritiska system?

Outsourcing av underhåll är en växande trend (Ali-Marttila et al., 2017; Murthy et al., 2015), bland annat för säkerhetskritiska system. Ett säkerhetskritiskt system kräver ökad säkerhet för att minska risken för oönskad informationsspridning som kan skada ekonomisk tillväxt (Bendovschi, 2015; Bishop, 2004). Underhåll är en aktivitet som bidrar till ökad säkerhet, då det identifierar avvikelser i system, vilket innebär att dessa kan åtgärdas i ett tidigt skede (Flodén, 2013). Underhåll av säkerhetskritiska system kräver expertkompetens som företag kan få tillgång till via outsourcing (Ali-Marttila et al., 2017; Murthy et al., 2015). En nackdel med outsourcing utifrån resultatet är att kunder inte delar nödvändig information med leverantören på grund av säkerhetsklassning. Att kunder inte är villiga att dela med sig av information, kan bero på rädsla för oönskad informationsspridning (Pereira et al., 2017). Vidare ställer det krav på relationen till kunden för att skapa trygghet och tillit, vilket kan uppnås genom ett nära samarbete (Christopher, 2016; Jansen, 2017). Nära samarbete anses vara viktigt för underhållsleverantörerna, vilket underlättar informationsdelning mellan parterna och är avgörande för att utföra underhållet på bästa möjliga sätt (Edgren & Skärvad, 2014). När information delas mellan företag kan blockchain vara ett alternativ, i syfte att öka säkerheten då aktiviteter i system synliggörs av samtliga parter (Skinner, 2016).

Ett problem som identifierats i resultatet är att kunder upplever förlorad kontroll när underhåll outsourcas. Detta innebär att underhållsleverantören, i samverkan med kunden, måste utvärdera säkerheten i realtid för att säkra kontroll (Boiko et al., 2018). Ytterligare ett alternativ för ökad kontroll är implementering av riktlinjer för att identifiera hot i ett tidigt skede, vilket uppnås genom ett informationssystem (Hallberg et al., 2017: Kaur & Sharman, 2017). Ett informationssystem möjliggör att leverantören och kunden kan kommunicera med varandra i realtid, vilket bidrar till att identifiera avvikelser, skydda aktiviteter och säkra nätverket mot obehörigt intrång (Heickerö, 2012). Underhållsleverantörer kan med fördel implementera en informationssäkerhetspolicy, i syfte att ge kunden kontroll över underhållet trots outsourcing (Bowin, 2004; Flowerday & Tuyikeze, 2016).

Resultatet påvisar att underhållsleverantörerna säkerställer uppfyllelse av kundkrav på olika sätt, vilket tros bero svårigheter att kontrollera kundkrav samt avsaknad av ett etablerat arbetssätt (Heickerö, 2012). Att efterleva kundkrav är avgörande för ett nära samarbete och tillit i relationen (Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav (Swedish Standards Institute, 2017)). Ett verktyg för att säkerställa efterlevnad av kundkrav är implementering av ISO 27001:2017, vilket bidrar till ett systematiskt arbetssätt för att säkerställa uppfyllelse av kundkrav och skapa förtroende (Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav (Swedish Standards Institute, 2017)). Implementering av en standard kräver kontinuerlig utvärdering, vilket på ett effektivt sätt kan utföras med PDSA-cykeln (Ammenberg, 2012).

Underhållsleverantörerna upplever risken för informationsspridning olika, däremot anses det generellt finnas en ökad risk för informationsspridning när underhåll av säkerhetskritiska system outsourcas. Detta tros bero på att flera system integreras i nätverket, vilket bidrar till svårigheter att säkerställa integritet och ställer krav på ökad säkerhet för att skydda data (Jansen, 2017; Oesterreich & Teuteberg, 2016; Santos et al., 2017; Vaidya et al., 2018). Utifrån ett kundperspektiv är det avgörande att underhållsleverantören förmår att skydda data och information, då informationsspridning kan leda till negativ ekonomisk påverkan (Bendovschi, 2015; Heickerö, 2012; Pereira et al., 2017; Zegzhda et al., 2018). ISO 27001:2017 anses bidra till god kommunikation mellan parterna vad gäller säkerhet, i syfte att skapa förståelse, kontroll och tydliga riktlinjer. Underhållsleverantörerna har ett avtal med kunder, vilket anses vara av stor vikt för att minska risken för informationsspridning. Vidare bidrar ett avtal till ökat förtroende och kontroll samt fördelar ansvar vid oönskad informationsspridning (Bowin, 2004).

5.2 Tillverkande företag

Företag	4	5	6	7	8	9	10	11
Finns det säkerhetskritiska system?	Ja	Ja	Ja	Ja	Ja	Ja	Ja	Ja
Krävs underhåll av systemen? Vad?	Patchingar, enhancements	Ja	Komponentbyten, programmering, uppdatering	Ja	Ja	Uppdatering, uppgraderingar	Uppdateringar, uppgraderingar	Systemövervakning, resurshantering, stöd, ständig förbättring
Outsourcas underhåll av säkerhetskritiska system?	Nej	Nej	Nej	Nej	Ja	Ja/Nej	Ja	Ja
Varför/Varför inte?	Resurser, kontroll	Ej behov, kompetens	Kontroll, kompetens	Kontroll	Kostnadsfördelar	Kostnadseffektivitet, leveransfrågor, kompetens	Kompetens	Resurstillgång, kompetens, kostnadsfördelar, legala krav, samverkan, relationer
Finns det nackdelar med att utföra underhåll internt?	Svårt att anpassa resurser till varierat behov	Inga nackdelar	Svårt att underhålla kompetens	Inga nackdelar	N/A	Begränsad kompetens	N/A	N/A
Outsourcas hela/delar av underhåll?	N/A	N/A	N/A	N/A	Hela	Delar	Delar	Hela
När utförs underhåll?	N/A	N/A	N/A	N/A	Hela tiden	Vid behov	Vid behov	Hela tiden
Påverkas relationen av att det är underhåll av ett säkerhetskritiskt system som outsourcas?	N/A	N/A	N/A	N/A	Internationell leverantör – språk, armlängds avstånd	Påverkas inte	Hårdare krav, bakgrundkontroll, nära samarbete	Större omfattning, väl genomtänkt avtal, förtydligande, dokumentation, välutvecklade system
Finns det problem i leverantörsrelationen?	N/A	N/A	N/A	N/A	Inte fördelat ansvar över uppföljningar vid systemuppdatering	Konkurrenssynpunkt	Uppfyllelse av servicegrad	Tillit, bristfällig information
Vad krävs för en bra leverantörsrelation?	N/A	N/A	N/A	N/A	God kommunikation, snabb respons vid förändringar	Nära samarbete, ej beroendeställning	Struktur, beskrivet tillvägagångssätt, påverkande parametrar, provkörningar i systemet	Tillit, proaktivitet, innovativt tänkande, ständig förbättring
Hur säkerställs att leverantören efterlever krav?	N/A	N/A	N/A	N/A	Utvärdering av varje enskilt fall	Mål, uppföljning & öppen dialog	Svårt, kräver insyn & kompetens	Teambaserat arbete
Är informationsspridning en kritisk faktor?	N/A	N/A	N/A	N/A	Ej angivet	Nej	Ja	Ja
Finns det en ökad risk för informationsspridning?	N/A	N/A	N/A	N/A	Ej angivet	Nej	Ja	Ja
Finns det kontroll över informationsspridning?	N/A	N/A	N/A	N/A	Ej angivet	Nej	Begränsad	Ja
Hur bevaras kontroll över processer?	N/A	N/A	N/A	N/A	Ej angivet	Styrande i relationen till leverantören	Äger program & kod	Genom samarbete med underhållsleverantören
Hur ser avtalet ut till leverantören, ansvar vid informationsspridning?	N/A	N/A	N/A	N/A	Parten som sprider information bär ansvar	Ej angivet	Reglerat avtal	Sekretessavtal

Tabell 3: Tabellen illustrerar en cross-case analys av resultatet från tillverkande företag.

5.2.1 Vilka är de kritiska faktorerna för att behålla kontroll vid outsourcing av underhåll för säkerhetskritiska system?

Resultatet visar att alla tillverkande företag har säkerhetskritiska system, vilket innebär en ökad osäkerhet vad gäller säkerhet (Carlsson & Jacobsson, 2012; Pereira et al., 2017). Fyra av företagen som deltagit i studien outsourcar underhåll av säkerhetskritiska system med orsak av kostnader och tillgång på extern kompetens. Företag som valt att utföra underhåll internt gör det med orsak av tillgång till interna resurser, kontroll och kompetens, där kontroll är den avgörande faktorn till beslutet (Boiko et al., 2018). En faktor som talar emot outsourcing är den ökade risken för informationsspridning (Ashibani & Mahmoud, 2017; Yeboah-Ofori & Islam, 2019; Zegzhda et al., 2018). Trots ökad risk för informationsspridning vid outsourcing anses ny teknik bidra till kontroll eftersom det möjliggör kommunikation och identifiering av avvikelser i system (Edgren & Skärvad, 2014; Hagberg & Henriksson, 2018; Vaidya et al., 2018).

Något som utmärker sig i studiens resultat är att både traditionell leverantörsrelation och ett nära samarbete råder vid outsourcing av underhåll för säkerhetskritiska system. Det anses vara fördelaktigt att ha ett nära samarbete med underhållsleverantören när det handlar om säkerhetskritiska system, vilket även tros minska risken för oönskad informationsspridning (Christopher, 2016). Trots att traditionell leverantörsrelation förekommer nämns inte detta i respondenternas beskrivning av en god leverantörsrelation. Samtliga respondenter har en tydlig bild av en god leverantörsrelation bör innefatta, däremot tycks det vara svårt att verkställa visionen. För att uppnå en bra leverantörsrelation bör denna bygga på god kommunikation, tillit och ett nära samarbete (Christopher, 2016; Edgren & Skärvad, 2014). Vidare anses det vara avgörande att företagen utvecklar ett nära samarbete med leverantören för att undvika leverantörsproblemen som resultatet påvisar (Christopher, 2016; Edgren & Skärvad, 2014).

Resultatet påvisar att kompetens är en avgörande faktor vid valet att outsourca underhåll av säkerhetskritiska system (Ali-Marttila et al., 2017; Edgren & Skärvad, 2014; Hagberg & Henriksson, 2018; Murthy et al., 2015). Kompetens gällande informationssäkerhet är avgörande för att minska risken för oönskad informationsspridning där outsourcing är fördelaktigt då det möjliggör ett utbyte av kunskap (Bowin, 2004; Hagberg & Henriksson, 2018; Hallberg et al., 2017). Flera av respondenterna upplever en ökad risk för

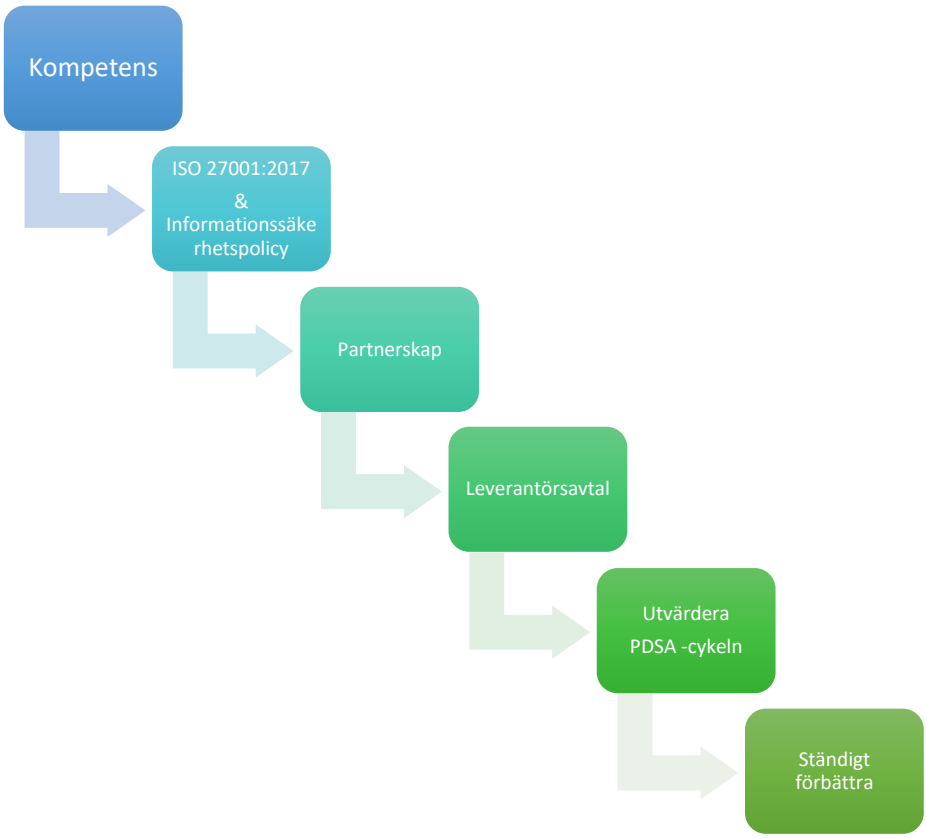
informationsspridning med orsak av att underhållet gäller säkerhetskritiska system. En orsak till att säkerhetsnivåer upplevs olika kan vara tolkningen av säkerhetsbegreppet, vilket påverkas av företagskultur (Hallberg et al., 2017; Oestrreich & Teuteberg, 2016; Vaidya et al., 2018). Ett etablerat arbetssätt anses bidra till att risken för informationsspridning minskar, förslagsvis genom att implementera ett säkerhetssystem som möjliggör identifiering av specifika händelser och obehörigt intrång (Bishop, 2004). Samtliga företag har ett leverantörsavtal för att minska risken för informationsspridning, då det inkluderar parten som bär ansvar vid informationsspridning, reglerat avtal och sekretessavtal. Ett sekretessavtal anses fördelaktigt när underhåll av säkerhetskritiska system outsourcas då det reglerar säkerhetsvillkor, beaktar informationsspridning och ansvarsfördelning (Hagberg & Henriksson, 2018; Bowin, 2004). För en framgångsrik hantering av ett outsourcingavtal kan ett informationssystem användas, vilket ger stöd samt skapar förutsättningar för samverkan och informationsdelning mellan parter (Flodén, 2013; Van Niekerk & Visser, 2010). Resultatet påvisar att samtliga företag säkerställer kravuppfyllelse på liknande sätt, i form av målsättning, utvärdering, teambaserat arbete och öppna dialoger. För att säkerställa att kraven efterlevs kan företagen implementera en strukturerad utvärdering genom PDSA-cykeln.

Ytterligare arbetssätt för att minska risken för oönskad informationsspridning är implementering av en informationssäkerhetspolicy, i syfte att tydliggöra vad som ska skyddas, ansvarsfördelning, utförande och hur incidenter ska hanteras (Bowin, 2004). Ansvarsfördelning nämns i resultatet som en problematisk faktor vad gäller leverantörsrelationen, vilket påvisar behovet av en informationssäkerhetspolicy för att skapa medvetenhet, förståelse och tydliga riktlinjer. En informationssäkerhetspolicy hjälper företaget att lyfta säkerhetsfrågor såväl inom företag som med externa partners, i syfte att minska risken för oönskad informationsspridning (Carlsson & Jacobsson, 2012; Pereira et al., 2017). För att stärka arbetet med säkerhet och minska risken för informationsspridning kan företaget implementera ISO 27001:2017, vilket bidrar till ett systematiskt arbetssätt (Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav (Swedish Standards Institute, 2017)). ISO 27001:2017 innefattar utförande av riskanalyser, vilket är viktigt för att undvika informationsspridning (Bowin, 2004). När företag implementerar en standard är det viktigt att utvärdera arbetet kontinuerligt för att identifiera behov av förändringar, där PDSA-cykeln är ett effektivt tillvägagångssätt (Ammenberg, 2016).

5.2.2 Hur kan de identifierade kritiska faktorerna hanteras i verksamheten?

Företags val att outsourca underhåll anses vara fördelaktigt av viss litteratur (Carlsson & Jacobsson, 2012), medan andra förklarar att det bidrar till ökad risk för informationsspridning (Heickerö, 2012). Oavsett om ett företag väljer att outsourca underhåll eller inte har denna studie lett fram till arbetssätt och metoder för att minska risken för informationsspridning. Resultatets cross-case analys har bidragit till identifiering av kritiska faktorer när underhåll av säkerhetskritiska system outsourcas. Kritiska faktorer för informationsspridning är kompetens, kontroll, nära samarbete, tillit, god kommunikation, efterlevnad av kundkrav samt god kännedom om verksamheten. Utifrån studiens analys har flera tillvägagångssätt identifierats, vilka bygger på de kritiska faktorerna, i syfte att minska risken för informationsspridning. Vidare har tillvägagångssätten placerats i en modell där ordningsföljden är avgörande i syfte att bygga upp säkerhetsarbetet från grunden. Modellen anses fördelaktig då det bidrar till att förankra säkerhetsarbetet i verksamheten och bygger på att stegen utförs i kronologisk ordning för att uppnå dess maximala kapacitet.

Figur 2: Figuren illustrerar ett tillvägagångssätt för att säkerställa kontroll av informationsspridning vid outsourcing av underhåll för säkerhetskritiska system.



Kompetens (1) är avgörande för att etablera säkerhetsarbetet i företag såväl externt som internt. Det är viktigt att medarbetarna har kompetens, förståelse och medvetenhet för säkerhet och risker, då bristande kompetens kan leda till säkerhetsincidenter (Hallberg et al., 2017). För ett erhålla kompetens föreslås samarbete med externa aktörer, där kunskap kan delas mellan parter i syfte att ständigt utveckla kompetens (Ali-Marttila et al., 2017; Bowin, 2004; Murthy et al., 2015). För att erhålla kunskap föreslås även branschstandarden ISO 27001:2017 och att implementera en informationssäkerhetspolicy.

Informationssäkerhetspolicy & ISO 27001:2017 (2) används för att förmedla riktlinjer och bidrar till att skapa kännedom om verksamheten för såväl medarbetare som underhållsleverantören (Bowin, 2004). ISO 27001:2017 används för att uppfylla organisationens informationssäkerhetskrav och en informationssäkerhetspolicy förmedlar hur arbetet ska bedrivas vad gäller säkerhet. Det är av stor vikt att verktygen förankras med leverantören för att säkerställa god kännedom hur säkerhetsarbetet ska bedrivas, i syfte att minska risken för oönskad informationsspridning.

Partnerskap (3) är viktigt för att minska risken för informationsspridning och behålla kontrollen vid outsourcing (Christopher, 2016; Jansen, 2017). Vidare är partnerskap avgörande för att företag ska dela med sig av nödvändig information till leverantörer, vilket påverkar förmågan att uppfylla kundkrav. Ett partnerskap kan uppfyllas genom ett nära samarbete, tillit och god kommunikation med leverantören (Christopher, 2016; Edgren & Skärvad, 2014).

Leverantörsavtal (4) minskar risken för informationsspridning samt bidrar till ökat förtroende och kontroll (Bowin, 2004). Ett leverantörsval ska inkludera säkerhetsvillkor, beakta informationsspridning och beskriva vem som bär ansvar vid oönskad informationsspridning.

Utvärdering (5) är ett viktigt steg som säkerställer att säkerhetsarbetet bedrivs enligt förväntningar. PDSA-cykeln är ett verktyg som ska används för att utvärdera aktiviteter i verksamheten, vilket möjliggör ständig förbättring av kompetens, leverantörsavtal, informationssäkerhetspolicy & ISO 27001:2017 samt leverantörsrelationen (Ammenberg, 2016).

Ständig förbättring (6) bidrar till att minska risken för informationsspridning och att säkerhetsarbetet är anpassat till rådande omständigheter. Företag ska arbeta med ständig förbättring i syfte att uppnå ekonomisk tillväxt och social hållbarhet (Ammenberg, 2012), då informationsspridning kan leda till förlorad inkomst (Pereira et al., 2017). Företag ska ständigt förbättra säkerhetsarbetet för att säkerställa långsiktig hållbarhet både vad gäller ekonomisk tillväxt och samhället (Globala målen, 2019).

6. Slutsats

Syftet med studien var att undersöka hur organisationer kontrollerar informationsspridning vid outsourcing av underhåll för säkerhetskritiska system. En cross-case analys av studiens resultat identifierade kritiska faktorer för informationsspridning när underhåll outsourcas. Studiens analys bidrog till att finna verktyg och arbetssätt för att minska risken för informationsspridning, vilket resulterade i en modell. Resultatet har påvisat att företag i dagsläget inte upplever kontroll av informationsspridning som ett problem. Industrins utveckling mot digitalisering och automatisering tros däremot bidra till ökad risk för informationsspridning, vilket studien belyser. Studiens modell har inte testats i en verksamhet, vilket bör göras i framtiden. För vidare forskning kan området med fördel studeras i en större omfattning och inkludera andra branscher, i syfte att öka resultatets generaliserbarhet. Det kan vara aktuellt att studera blockchain i samband med outsourcing av underhåll för säkerhetskritiska system i framtiden, då det finns ett samband mellan blockchain och informationsspridning.

Referenser

Ali-Marttila, M., Marttonen-Arola, S., Kärri, T., Pekkarinen, O., & Saunila, M. (2017). Understand what your maintenance service partners value. *Journal of Quality in Maintenance Engineering*, *23*(2), 144-164. doi:10.1108/JQME-08-2016-0035

Ammenberg, J. (2012). *Miljö- och hållbarhetsarbete i företag och andra organisationer* (2:4). Lund: Studentlitteratur AB.

Ashibani, Y., & Mahmoud, Q, H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *In Computers & Security 68*, 81-97. doi:10.1016/j.cose.2017.04.005

Bendovschi, A. (2015). Cyber Attacks - Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance, 28*(2015), 24-31. doi: 10.1016/S2212-5671(15)01077-1

Bengtsson, L., Berggren C., & Lind, J. (2005). *Alternativ till outsourcing* (1:1). Malmö: Liber AB.

Bishop, M. (2004). *Introduction to Computer Security*. Boston: Addison-Wesley Educational Publishers Inc.

Blomkvist, P., & Hallin, A. (2014). *Metod för teknologer: Examensarbete enligt 4-fasmodellen* (1:3). Lund: Studentlitteratur AB.

Boiko, A., Shendryk, V., & Boiko, O. (2018). Information systems for supply chain management: uncertainties, risks and cyber security. *Procedia Computer Science, 149*(2019), 65-70. doi:10.1016/j.procs.2019.01.108

Bowin, J. (2004). *Ge din information rätt säkerhet, Handbok i informationssäkerhet.*Stockholm: SIS Förlag.

Bryman, A. (2011). Samhällsvetenskapliga metoder (2:3). Malmö: Liber AB.

Carlsson, B., & Jacobsson, A. (2012). *Om säkerhet i digitala ekosystem* (1:1). Lund: Studentlitteratur AB.

Chaim, O., Muschard, B., Cazarini, E., & Rozenfeld, H. (2018). Insertion of sustainability performance indicators in an industri 4.0 virutal learning environment. *Procedia Manufacturing, 21*(2018), 446-453. doi:10.1016/j.promfg.2018.02.143

Christopher, M. (2016). *Logistics and Supply Chain Management* (5). United Kingdom: Pearson Education.

Dhillon, G., Syed, R., & Sá-Soares, D. F. (2016). Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors. *Information & Management, 54*(2017), 452-464. doi:10.1016/j.im.2016.10.002

Durst, S., & Edvardsson, I. R. (2012). Knowledge management in SMEs: a literature review. *Journal of Knowledge Management, 16*(6), 879-903. doi:10.1108/13673271211276173

Edgren, J., & Skärvad, P. (2014). *Nätverksorganisationer - outsourcing, partnerskap och nya organisationer* (2). Stockholm: Liber AB.

Flodén, J. (2013). *Essential of information systems* (1:1). Lund: Studentlitteratur AB.

Flowerday, V. S., & Tuyikeze, T. (2016). Information sercurity policy development and implementation: The what, how and who. *Computers and security, 61*(2016), 169-183. doi: 10.1016/j.cose.2016.06.002

Globala målen. (2019). Hållbar industri, innovationer och infrastruktur. Hämtad från 2019-04-17 från https://www.globalamalen.se/om-globala-malen/mal-9-hallbar-industri-innovationer-och-infrastruktur/

Gollmann, D. (2011). *Computer Security* (003). Chichester: John Wiley & Sons, Ltd.

Hagberg, L., & Henriksson, T. (2018). *Underhåll i världsklass* (2). Lund: OEE Consultants AB.

Hallberg, J., Johansson, P., Karlsson, F., Lundberg, F., Lundgren, B., & Törner, M. (2017). *Informationssäkerhet och organisationskultur* (1:1). Lund: Studentlitteratur AB.

Heickerö, R. (2012). *Internets mörka sidor - Om cyberhot och informationskrigsföring.* Riga: Livonia Print

Jansen, C. (2017). Stabilizing the Industrial System: Managed Security Services' Contribution to Cyber-Peace. *IFAC PapersOnLine, 50-1*(2017), 5155-5160. doi:10.1016/j.ifacol.2017.08.786

Kaur, K. & Sharma, R. (2017). Critical: Threat model for an outsourcing business. *International Conference on Computing, Communication and Networking Technologies (ICCCNT), 1,* 1-5. doi:10.1109/ICCCNT.2017.8204093

Langfield-Smith, K., & Smith, D. (2003). Management control systems and trust in outsourcing relationships. *Management Accounting Research, 14*(3), 281-307. doi:10.1016/S1044-5005(03)00046-5

Laplante, P. A., & DeFranco, J. F. (2017). Software Engineering of Safety-Critical Systems: Themes From Practitioners. *IEEE Transactions on Reliability, 66*(3), 825-836. doi:10.1109/TR.2017.2731953

Lennerfors, T. T. (2019). *Etik för ingenjörer* (1). Lund: Studentlitteratur AB.

Mishra, D., Kumar, S., Sharma, R.R.K., & Dubey, R. (2017). Outsourcing decision: do strategy and structure really matter?. *Journal of Organizational Change Management, 31*(1), 26-46. doi: 10.1108/JOCM-04-2017-0144

Murthy, D. N. P., Karim, M. R., & Ahmadi, A. (2015). Data management in maintenance outsourcing. *Reliability Engineering and System Safety, 142,* 100-110. doi:10.1016/j.ress.2015.05.002

Oesterreich, D. T., & Teuteberg, F. (2016). Understanding the implications of digitisation and automation in the context of Industry 4.0: A triangulation approach and elements of a research agenda for the construction industry. *Computers in Industry, 83*(2016), 121-139. doi:10.1016/j.compind.2016.09.006

Patel, R., & Davidson, B. (2003). Forskningsmetodikens grunder (3). Lund: Studentlitteratur AB.

Pereira, T., Barreto, L., & Amaral, A. (2017). Network and information security challenges within Industri 4.0 paradigm. *Procedia Manufacturing, 13*(2017), 1253-1260. doi:10.1016/j.promfg.2017.09.047

Prajogo, D., & Olhager, J. (2011) Supply chain integration and performance: The effects of long-term relationships, information technology and sharing, and logistics integration. *Int. J. Production Economics 135*(2012), 514-522. doi:10.1016/j.ijpe.2011.09.001

Rojko, A. (2017). Industry 4.0 Concept: Background and Overview. *International Journal of Interactive Mobile Technologies, 11*(5), 77-90. doi:10.3991/ijim.v11i5.7072

Santos, C., Mehrsai, A., Barros, C. A., Ataújo, M., & Ares, E. (2017). Towards Industry 4.0: an overview of European strategic roadmaps. *Procedia manufacturing, 13*(2017), 972-979. doi:10.1016/j.promfg.2017.09.093

Saunila, M., Nasiri, M., Ukko, J., & Rantala, T. (2019). Smart technologies and corporate sustainability: The mediation effect of corporate sustainability strategy. *Computers in Industry, 108*(2019), 178-185. doi:10.1016/j.compind.2019.03.003

Skinner, C. (2016). *Valueweb: How Fintech Firms Are Using Mobile and Blockchain Technologies to Create the Internet of Value* (1:1). Singapore: Marshall Cavendish International.

Sohlberg, P., & Sohlberg, B. M. (2013). *Kunskapens former: Vetenskapsteori och forskningsmetod* (3:1). Stockholm: Liber AB.

Swedish Standards Institute. (2017). *Informationsteknik – Säkerhetstekniker – Ledningssystem för informationssäkerhet – Krav*. SS-EN ISO/IEC 27001:2017

Tidd, J., & Bessant, J. R. (2014). *Strategic Innovation Management.* Chichester: John Wiley & Sons, Ltd.

Vaidya, S., Ambad, P., & Bhosle, S. (2018). Industry 4.0 – A Glimpse. *Procedia Manufacturing, 20*(2018), 233-238. doi:10.1016/j.promfg.2018.02.034

Van Niekerk, A. J., & Visser, J. K. (2010). The role of relationship management in the successful outsourcing of maintenance. *South African Journal of Industrial Engineering, 21*(2), 79-90. doi:10.7166/21-2-51

Wangen, G., Snekkenes, E., & Hallstensen, C. (2017). A framework for estimating information security risk assessment method completeness. *International Journal of Information Security, 17*(6), 681-699. doi:10.1007/s10207-017-0382-0

Yeboah-Ofori, A., & Islam, S. (2019). Cyber Security Threat Modeling for Supply Chain Organizational Environments. *Future Internet, 11*(3), 3-25. doi:10.3390/fi11030063

Yin, K. R. (2012). *Applications of Case Study Research* (3). California: SAGE Publications, Inc.

Yin, K. R. (2009). *Case Study Research - Design and Methods* (4:5). California: SAGE Publications, Inc.

Zegzhda, D. P., Vasil'ev, Yu. S., & Poltavtseva, M. A. (2018). Approaches to Modeling the Security of Cyberphysical Systems. *Automatic Control and Computer Sciences, 52*(8), 1000-1009. doi:10.3103/S014641161808031X

Bilagor

Bilaga 1

Vi är två studenter som läser Industriell ekonomi på Högskolan i Gävle där vi just nu skriver vårt examensarbete. Examensarbetet syftar till att undersöka hur organisationer kontrollerar informationsspridning vid outsourcing av underhåll för säkerhetskritiska system. Studien ska även presentera en strategi för att säkerställa kontroll vid outsourcing. Vårt syfte grundas i att det i dagsläget finns ett forskningsgap gällande outsourcing och informationssäkerhet, vilket kan tänkas bero på snabba förändringar på marknaden och förändrad industri mot automatisering och digitalisering. Vi vet att det idag finns problem inom industrin att säkra kontroll över informationsspridning när företag outsourcar aktiviteter, därför tror vi att detta arbete är mycket intressant för industrin som bransch.
För att undersöka området behöver vi er hjälp att svara på några intervjufrågor, vilket tar ca. 15 minuter. Ni kommer att vara helt anonyma som företag och respondent och när arbetet är klart i mitten på juni kommer ni att få ta del av detta.

Intervjuunderlag 1

1. **Har ni säkerhetskritiska system? (ett system som innehåller information och data som är kritisk för verksamhetens fortlöpande)**

Svar:

2. **Vad är det för typ av system som är säkerhetskritiskt för er?**

Svar:

3. **Kräver detta/dessa system någon form av underhåll?**

Svar:

4. **Outsourcar ni underhåll av säkerhetskritiska system?**

Svar:

Om Nej, besvara frågorna 5 och 6, om Ja, besvara frågorna 7–18.

5. **Om nej, varför inte? Finns det några huvudfaktorer som påverkat beslutet?**

Svar:

6. **Anser du att det finns nackdelar att i egen regi utföra underhåll av säkerhetskritiska system?**

Svar:

7. **Outsourcas hela underhållet av systemen eller är det vissa delar som outsourcas, vilka?**

Svar:

8. **Vilken typ av funktion fyller underhållsleverantören, sker underhåll hela tiden eller endast vid incidenter?**

Svar:

9. **Vad är det som påverkar valet att outsourca underhåll?**

Svar:

10. **Påverkas relationen till underhållsleverantören av att det är ett säkerhetskritiskt system som ska outsourcas? (Jämfört med om det är en annan aktivitet som ska outsourcas).**

Svar:

Om ja, på vilket sätt? (Nära samarbete eller en relation som hålls på en armlängds avstånd)

Svar:

11. **Har ni identifierat några problematiska faktorer i relationen till underhållsleverantören på grund av att det är ett säkerhetskritiskt system som ska hanteras? (Jämfört med om det är en annan aktivitet som ska outsourcas).**

Svar:

12. **Vad anser du är viktigt i en leverantörsrelation när underhåll av ett säkerhetskritiskt system outsourcas? (Speciellt kontrakt på grund av känslig information?)**

Svar:

13. **Hur säkerställer ni att leverantören uppfyller de krav som ställs?**

Svar:

14. **Är informationsspridning en kritisk faktor i er verksamhet?**

Svar:

15. **Finns det en ökad risk för informationsspridning när underhåll av säkerhetskritiska system outsourcas?**

Svar:

16. **Har ni kontroll över informationsspridning när underhåll outsourcas av ett säkerhetskritiskt system?**

Svar:

17. **Hur arbetar ni för att bevara kontroll över processerna när underhåll av säkerhetskritiska system outsourcas?**

Svar:

18. Hur ser avtalet ut mellan er och underhållsleverantören vad gäller ansvar vid oönskad informationsspridning?

Vem bär ansvaret vid eventuell spridning av information?

Svar:

Kontaktuppgifter för återkoppling:

Namn:

Mailadress:

Tack för din medverkan!

Med vänliga hälsningar,

Maja Myr och Louise Törnell

Bilaga 2

Vi är två studenter som läser Industriell ekonomi på Högskolan i Gävle där vi just nu skriver vårt examensarbete. Examensarbetet syftar till att undersöka hur organisationer kontrollerar informationsspridning vid outsourcing av underhåll för säkerhetskritiska system. Studien ska även presentera en strategi för att säkerställa kontroll vid outsourcing. Vårt syfte grundas i att det i dagsläget finns ett forskningsgap gällande outsourcing och informationssäkerhet, vilket kan tänkas bero på snabba förändringar på marknaden och förändrad industri mot automatisering och digitalisering. Vi vet att det idag finns problem inom industrin att säkra kontroll över informationsspridning när företag outsourcar aktiviteter, därför tror vi att detta arbete är mycket intressant för industrin som bransch.

För att undersöka området behöver vi er hjälp att svara på några intervjufrågor, vilket tar ca. 15 minuter. Ni kommer att vara helt anonyma som företag och respondent och när arbetet är klart i mitten på juni kommer ni att få ta del av detta.

Intervjuunderlag 2

1. **Hur många företag inom industribranschen är ni leverantörer åt, vad gäller underhåll av säkerhetskritiska system? (ett system som innehåller information och data som är kritisk för verksamhetens fortlöpande)**

   Svar:

2. **Påverkas relationen till kunden av att det är underhåll av ett säkerhetskritiskt system som ska outsourcas? (Jämfört med om det är en annan aktivitet som ska outsourcas).**

   Svar:

3. **Om ja, på vilket sätt? (Nära samarbete eller en relation som hålls på en armlängds avstånd)**

   Svar:

4. **Vad anser du är viktigt i en kundrelation när underhåll av ett säkerhetskritiskt system outsourcas? (Speciellt kontrakt på grund av känslig information?)**

   Svar:

5. **Har ni identifierat några problematiska faktorer i relationen till kunden på grund av att det är ett säkerhetskritiskt system som hanteras? (Jämfört med om det är en annan aktivitet som ska outsourcas till er).**

   Svar:

6. **Outsourcas hela underhållet av systemen eller är det vissa delar som outsourcas, vilka?**

   Svar:

7. **Vilken typ av funktion fyller ni som underhållsleverantör, sker underhåll hela tiden eller endast vid incidenter?**

   Svar:

8. **Hur säkerställer ni att krav från kunder uppfylls?**

   Svar:

9. **Finns det en ökad risk för informationsspridning när underhåll av säkerhetskritiska system outsourcas?**

   Svar:

10. **Om ja, hur arbetar ni för att hantera kontroll över informationsspridning?**

    Svar:

11. **Hur ser avtalet ut mellan er och kunden vad gäller ansvar vid oönskad informationsspridning? Vem bär ansvaret vid eventuell spridning av information?**

    Svar:

Kontaktuppgifter för återkoppling:

Namn:

Mailadress:

Tack för din medverkan!

Med vänliga hälsningar,

Maja Myr och Louise Törnell