tillväxt verket

Digitala affärsrisker

Kunskapsöversikt av riskmedvetenhet och informations- och cybersäkerhetsarbete i små och medelstora företag

Rapport 0340

Tillväxtverkets publikationer kan laddas ner på tillvaxtverket.se. Vill du beställa en tryckt publikation eller söker du en publikation som publicerades innan 2015 hänvisar vi till vår webbshop

Stockholm, Oktober 2020
ISBN digital: 978-91-88961-70-9
Rapportnummer: 0340

Har du frågor om denna publikation, kontakta:
Karin Östberg
Telefon, växel 08-681 91 00

Förord

Tillväxtverket arbetar för att stärka företagens konkurrenskraft. Genom kunskap, nätverk och finansiering skapar vi bättre förutsättningar för befintliga och framtida företag och attraktiva regionala miljöer där företag utvecklas.

Ett sätt att stärka affärsverksamheten är genom företagens arbete med informations- och cybersäkerhet. Den ökade globaliseringen och digitaliseringen innebär också ökade risker. Med nya tekniker kommer arbetet med cybersäkerhet och riskhantering bli en viktig framgångsfaktor för företagen och ha stor betydelse för en lyckad hållbar digitalisering och en fortsatt tillväxt.

Tillväxtverket fick 2018 ett regeringsuppdrag för att höja kompetensen inom digitalisering i små företag. Huvudsyftet är att stärka små företags digitala konkurrenskraft ur ett ekonomiskt och affärsmässigt perspektiv.

På uppdrag av Tillväxtverket genomförde IT-Säkerhetsbolaget och Sweco hösten 2019 denna studie. Huvudförfattare är Anna Kamf och Fredrik Jonasson, IT-Säkerhetsbolaget och Lisa Sjölund, Sweco. Arbetet skedde i dialog med Tillväxtverket. Rapporten är i denna version något kortad och något bearbetad. Rapportförfattarna står för sakinnehåll, slutsatser och rekommendationer.

I rapporten redovisar författarna för kartläggningar och analyser av utbud och efterfrågan på marknaden för informations- och cybersäkerhet, pekar på bristen på digital spetskompetens, gör en genomgång av lagstiftning och juridik inför området samt en internationell utblick. Den innefattar också en mindre enkät och djupintervjuer med företagare - om behov, efterfrågan och medvetenhet avseende strategier för digitalisering och digitala risker.

Förhoppningen är att denna studie och kartläggning ska bidra till ökade insikter om små och medelstora företags behov av ett systematiskt arbete med it-, cybersäkerhets- och informationssäkerhet.

Oktober 2020

Tim Brooks
Avdelningschef
Tillväxtverket

Karin Östberg
Projektledare
Tillväxtverket

1 Sammanfattning

Informationssäkerhet – ett försummat ämne bland tillväxtföretag

Då en stor del av informationen och tillgångarna är digitala ökar risken för dataintrång och andra digitala hot. Många företag känner inte till dessa risker men gör inget för att förhindra dem, vilket gör dem sårbara.

Generell låg medvetenhet hos företagen om digitala risker – oavsett digitaliseringsgrad i företagen

Medvetenheten om hot och risker är låg hos mindre företag, men det ställs heller få eller inga generella krav från myndigheter, kunder och företagsfrämjare avseende arbete med informationssäkerhet. De företag som arbetar strukturerat med informationssäkerhet gör det oftast om det finns sektorsspecifika lagkrav, när kunden kräver ett informationssäkerhetsarbete eller när de själva råkat ut för dataintrång och cyberattacker.

Inget tydligt samband mellan digital mognad och ökad riskmedvetenhet

Företagens utsatthet för digitala risker är tätt kopplat till deras nivå av digitalisering. Affärsmodeller som uteslutande existerar på internet, kanske också på en internationell marknad, är självklart mer känsliga för cyberattacker och borde ha en större beredskap. Det verkar inte finnas ett tydligt samband mellan att en högre digital mognad också leder till en ökad riskmedvetenhet och förståelse för de digitala riskerna i företaget. Detta är slutsatsen av en mindre företagsenkät och djupintervjuer med företagare.

Utbud inom informations- och cybersäkerhet finns men är inte känt och troligen inte anpassat för mindre företags behov

Det finns information och erbjudanden på marknaden som både den offentliga och privata verksamheten tillhandahåller, exempelvis av Myndigheten för samhällsskydd och beredskap, MSB, och Stöldskyddsföreningen. Flertalet privata aktörer erbjuder både konsulthjälp och certifieringar inom området. Få erbjudanden verkar vara anpassade till små och medelstora företags lite mer avancerade affärsmodeller.

Bristande grundkunskaper hos företagsfrämjarna

Många nystartade företag har företagsfrämjare som första kontakt. Grundkunskaperna inom informationssäkerhet hos företags- och innovationsfrämjare får ses som förhållandevis låga. Detta hänger delvis ihop med att de inte uppfattar frågorna som en del av deras uppdrag. Det finns förstås också ett samband till de ibland bristande kunskaperna och kompetensen om digitalisering rent generellt. Att utvärdera företagens risker är dock en central del i mångas arbete.

Säkerhet är inte ett krav vid val av system- och tjänsteleverantörer

Det viktigaste vid val av digitala system enligt de flesta företagen är funktionalitet, användarvänlighet och långsiktighet. Tillgängligheten är också viktig, vilket innebär att allt fler väljer molntjänster. Vid användande av molntjänster finns dock en tilltro till att molnleverantören hanterar alla aspekter av informationssäkerhet och cybersäkerhet. Många gånger levereras en generell lösning som ska vara kostnadseffektiv och passa alla, snarare än specifika säkerhetslösningar för företagen.

Bristen på informationssäkerhetskompetens i ledningen är en risk

Kartläggningen visar att kompetensen inom informationssäkerhet i ledning och styrelse är låg eller obefintlig. Ledningen litar antingen på en speciellt utsedd funktion i företaget, oftast IT, eller på hostingföretag och systemleverantörer. Några har god eller hög kompetens för att det är något som krävs av dem eller för att de är intresserade av informationssäkerhet.

Idag är det exempelvis lätt att beställa IT-system. Det behövs inte längre en IT-säkerhetschef eller liknande, vilket medför att vissa frågor inte kravställs innan system köps in.

GDPR en väckarklocka för ledningar och styrelser

GDPR har väckt frågan om informationssäkerhet och digitala risker i många styrelser och ledningsgrupper, men styrelsen har inte alltid förmågan att omvandla medvetenheten om risker till praktiska åtgärder. Medvetenheten i företagsledningar kring cybersäkerhetsfrågor ökar, dock är det framförallt i större organisationers styrelser. Tendensen från intervjuerna är att små tillväxtföretags ledningar ofta saknar denna medvetenhet.

Vad händer i EU?

EU arbetar med att öka EU-ländernas förmåga att hantera cyberangrepp bland annat genom det nya ramverket ”Cybersecurity Act” som handlar om att införa ett gemensamt certifieringssystem av tjänster, system och utrustning inom IT-området. För små och medelstora företag samtstartups innebär certifieringen minskade hinder för marknadsinträden, ett certifikat som "passar alla" i hela EU och giltigt i såväl privat som offentlig sektor. Certifierade lösningar kommer att ha en konkurrensfördel. Förhoppningen på sikt är att mindre tillväxtföretag därmed ska kunna konkurrera med de större företagen.

Kunskapshöjande insatser, ett sätt att hjälpa tillväxtföretag till en större medvetenhet och förändringar

Medvetenheten i samhället och i företagsledningar kring cybersäkerhetsfrågor ökar, särskilt viktig är frågan i större organisationers styrelser. En utmaning är dock att få små och medelstora företag, och särskilt tillväxtföretagen att börja agera.

Kunskapshöjande insatser bör vara riktade mot de aktörer som startups och tillväxtbolag först kommer i kontakt med; företagsfrämjare, inkubatorer och branschorganisationer. Hos dem bör medvetenheten och kompetensen höjas och krav ställas på att cybersäkerhetsfrågor och digitala risker ska ingå som en del av ordinarie rådgivning.

Förslag på insatser:

- Verka för att öka kunskapen om informations- och cybersäkerhet inkl digitala risker hos ledning och styrelser i företagen genom riktad utbildning av och hos företagsfrämjarna i form av seminarier, frukostmöten och företagsevent. Syftet med dessa aktiviteter är att ”Lära lärarna”. Om företagsfrämjare och andra aktörer ställer krav på att informations- och cybersäkerhet ska hanteras blir dessa frågor naturligt integrerade precis som frågor om ekonomi, kvalitet och miljö.

- Skapa cybersäkerhetsprogram/”sandlådor” för innovation och informationssäkerhet, utformat för att stötta små företag eller tillväxtföretag när de utvecklar innovativa produkter och tjänster.

Innehåll

2 Inledning

Denna studie och kartläggning har till syfte att vara ett kunskapsunderlag inom ramen för Tillväxtverkets regeringsuppdrag *"Uppdrag att utveckla och genomföra ett program för att höja kompetensen kring digitalisering i små företags ledningar och styrelser"* (Regeringen, 2018a). Uppdraget ska också kunna peka ut riktningen för framtida satsningar inom relaterade utvecklingsområden.

Uppdraget redovisar olika typer av digitala affärsrisker med fokus på informations- och cybersäkerhet och vilka behov och efterfrågan små tillväxtföretag har. Kartläggningen identifierar även vad den svenska marknaden erbjuder i form av information, stöd och rådgivning relaterat till informations- och cybersäkerhet.

Digitalisering är en förbättring kring nyttjandet av informationsteknologi i flera steg av den kommersiella och operativa verksamheten. Med teknikutveckling skapas möjligheter och introducerar, exempelvis Big Data, Internet of Things (IoT), Artificiell Intelligens (AI), vilket ger möjligheter att hitta innovativa lösningar som automatiserar och effektiviserar verksamheten. Allt blir uppkopplat, där olika system kommunicerar med varandra, vilket kan skap ett stort mervärde.

Samtidigt som digitalisering skapar möjligheter för affärsutveckling, skapar den även säkerhetsrisker som i och med den tekniska komplexiteten blir allt svårare att hantera. För att kunna hantera digitala säkerhetsrisker behövs en säkerhetskultur där informationssäkerhet finns med som en integrerad del i det dagliga arbetet och följer ett systems livscykel från idé till avveckling.

2.1 Vad är informationssäkerhet och cybersäkerhet?

Informationssäkerhet innebär att hantera information säkert genom att;

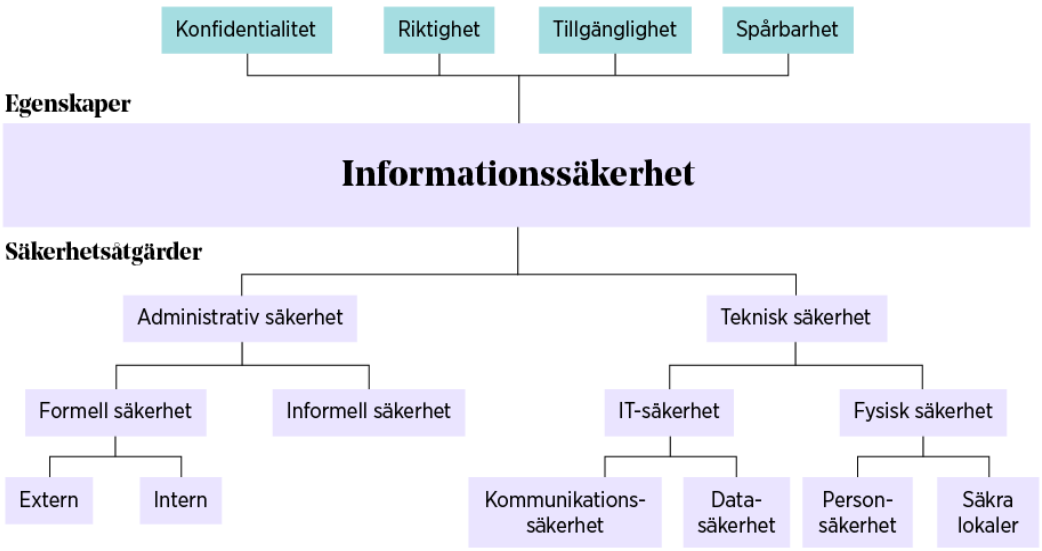
- Begränsa behörighet till information (konfidentialitet)
- Se till att information är korrekt och inte ändrad eller förstörd (riktighet)
- Information finns tillgänglig vid behov (tillgänglighet)

Informationssäkerhet innebär ett riskbaserat arbetssätt vid hantering av information samt införandet av de skyddsåtgärder och rutiner som behövs. Skyddsåtgärder ska vidare balanseras mellan skyddsvärdet, hot och kostnad, så kallad riskoptimering.

Informationstillgångar finns i många former, till exempel:

- Människor med sin kunskap och kompetens
- Lokaler
- Digital information
- Information på papper
- Ett samtal i en tågkupé

Figur 1 visar på vilka delar som ingår i begreppet informationssäkerhet vilket inkluderar både administrativ och teknisk säkerhet.



Figur 1: Informationssäkerhet innehåller flera delar, där säkerhetsåtgärder är både administrativ och teknisk säkerhet.

Genom ett systematiskt arbete med informationssäkerhet som bygger på etablerade standarder kan organisationer öka kvaliteten i och förtroendet för sin verksamhet. Informationssäkerhet omfattar både administrativa rutiner med policy och riktlinjer samt tekniskt skydd med bland annat brandväggar och kryptering. Det handlar om att ta ett helhetsgrepp och skapa en fungerande långsiktig process för att ge organisationens kritiska information det skydd som krävs utifrån krav från verksamheten, lagar, kunder och andra intressenter.

Ordet cybersäkerhet används ofta i svenskt språkbruk men har ingen entydig definition. Ofta avses ett företags arbete med IT-säkerhet. Ett försök till definition av ordets innebörd skulle kunna vara “försvar av datorer och servrar, mobila enheter, elektroniska system, nätverk och data mot skadliga angrepp”. Det kallas även informationstekniksäkerhet eller elektronisk informationssäkerhet. Termen är bred och omfattar allt från datorsäkerhet till katastrofåterställning och slutanvändarutbildning.

En av flera utmaningar är att hitta en gemensam definition av digital säkerhet som är giltig i samhällets samtliga domäner. I rapporten används ordet cybersäkerhet utifrån den definition som beskrivs i figur 2.

Digital security, cybersecurity, information security, cyber-defence, cybercrime: The need to simplify terminology

The multiplication of terms related to digital security in Swedish policy documents is an illustration of a maturing policy-making process. Sweden is not the only country in this situation as, unfortunately, there is no universally agreed terminology to capture the different facets of digital security in every context.

In its 2015 **Recommendation on Digital Security Risk Management for Economics and Social Prosperity**, the OECD uses the term "digital security" rather than "cybersecurity". OECD countries considered that "cybersecurity" was already used by different actors as a broad concept that did not reflect the multifaceted nature of this area. More generally, the favoured "digital" over "cyber" as the latter was used in certain circles as a synonym of "cyberwarfare", "cyberdefence" or "cyberinfluence".

Furthermore, "cyber" is absent from economic circles, which more generally stick to the digital semantic: digital economy, digital transformation, digitalization, etc. "Digital" facilitates the recognition of "digital security" as an economic issue by policy makers and business leaders. "Information security" was left aside as a technical management primarily reflecting the view of the techinal community (e.g. ISO/IEC 27000 "Information Security Management Systems" standards) rather than business leadership's perspective. It also carries ambiguity in an international context as it has a different scope in countries such as the People's Republic of China and the Russian Federation, which use it also to capture policies against disinformation, influence and information manipulation.

OECD rapport Going Digital Sweden 2018, s 117

Figur 2: Beskrivning av definition för cybersäkerhet. I denna rapport används ordet cybersäkerhet som beskrivs i rapporten OECD Going Digital Sweden.

2.2 Studiens uppdrag och syfte

Studien redovisar olika typer av digitala risker med fokus på informationssäkerhets- och cyberrisker och vilka behov och efterfrågan små tillväxtföretag har. Den redovisar även olika typer av stöd som finns på marknaden, nationellt och internationellt som kan användas av små företag. inkluderar en mindre kartläggning om hur digital kompetens kan bidra till ökad digital affärsutveckling i mindre företag, framförallt i tillväxtföretag. Slutligen redovisar studien rekommendationer för vilka kunskapshöjande insatser som behövs för att små tillväxtföretag strategiskt ska kunna utveckla säkra digitala affärsmodeller.

Följande tematiska områden utforskas i rapporten;

- Tema 1. Behov och efterfrågan av digitala affärsmodeller och strategier med särskilt fokus på digitala risker i små tillväxtföretag
- Tema 2. Kartläggning och analys av utbud och efterfrågan på marknaden avseende informations- och cybersäkerhet
- Tema 3. Lagstiftning och juridik
- Tema 4. Bristen på digital spetskompetens för affärsutveckling och ledarskapets roll
- Tema 5. Internationell utblick - informationskampanjer, vägledningar och guider

3 Metod för kartläggning

Kartläggningen inkluderar fem typer av datainsamlingsmetoder:

- Djupintervjuer
- Enkätintervjuer och webbenkät
- Skrivbordsstudie
- Intervjuer med företagsfrämjare
- Intervjuer med experter inom informations- och cybersäkerhet

I kartläggningen genomförs ingen branschspecifik redovisning eller analys utan en samlad bedömning av utbud, behov och efterfrågan gällande informationssäkerhet. Valet av branscher motiveras av ambitionen att fånga små och medelstora företag som har både högre respektive lägre digital mognad.

3.1 Datainsamlingsmetoder

För att komma i kontakt med företag för utskick av webbenkät har 1) företagskontakter beställts genom Bisnode och 2) för djupintervjuer har företag från sju företagsfrämjande organisationer kontaktats genom förslag från Tillväxtverket. Den så kallade snöbollsmetoden har applicerats vid kontakt med företag för djupintervjuer. Det innebär att vi har använt oss av kontakter för att bli hänvisade vidare till företag att intervjua.

När kontakt med företagen och företagsfrämjarna togs förklarades syftet med intervjun. En del av frågorna kan betraktas vara av känslig natur och därmed har respondenternas och företagens namn gjorts anonyma. Däremot anges företagens branschtillhörighet.

3.1.1 Djupintervjuer

Djupintervjuerna har varit mellan 30–50 minuter långa där en intervjuguide med frågor togs fram. Frågorna har förutom inledning och avslut delats upp i fyra fokusområden:

- Digitala affärsmodeller, -strategier och kunderbjudanden
- Lagstiftning och juridik
- Val av system- och tjänsteleverantörer
- Digital spetskompetens och ledarskapets roll

Det primära syftet med djupintervjuerna har varit att få en uppfattning av respondentens förståelse för och erfarenhet av digitala risker samt behov av informations-säkerhetsarbete.

3.1.2 Webbenkäter och telefonenkäter

Enkätintervjuer har genomförts via både webenkät och telefonenkät. Frågorna har delats in i samma tematiska fokusområden som djupintervjuerna.

3.1.3 Skrivbordsstudier

En skrivbordsstudie har genomförts för följande tematiska områden;

- Utbud informations- och cybersäkerhet
- Lagstiftning och juridik

- Digital spetskompetens och ledarskapets roll
- Nationell och internationell utblick

3.1.4 Intervjuer företagsfrämjare

Med företagsfrämjare innefattas företags-, affärs- eller innovationsfrämjare, såsom företagsrådgivare, inkubatorer och nyföretagarrådgivning. Alla intervjuade företagsfrämjare, utom Business Sweden och Nyföretagarcentrum, leder projekt i Tillväxtverkets regeringsuppdrag för Höjd digital kompetens kring små företags ledningar och styrelser.

Intervjuade företagsfrämjare var Almi Företagspartner Mälardalen, Business Sweden, GU Ventures, Företagarna, Halmstad Business Incubator/High Five, Nyföretagarcentrum och Stockholm Fashion District/Trade Partners Sweden

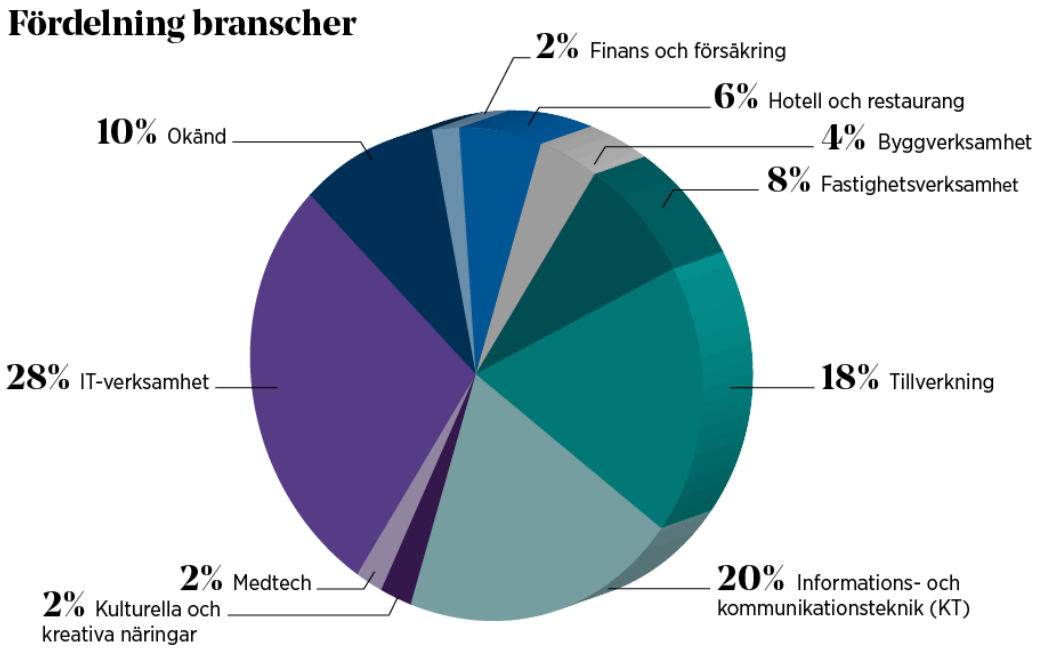
3.1.5 Intervjuer med experter

För att ytterligare belysa de slutsatser som framkommit har ett antal frågor sammanställts till två utvalda experter. De experter som deltagit i förstudien är Anne-Marie Eklund Löwinder, CISO på Internetstiftelsen och Åsa Schwartz, författare och cybersäkerhetsexpert. Anne-Maries och Åsas svar redovisas i separata faktarutor i rapporten.

4 Intervjuer och företagsenkät - branschfördelning

De 20 intervjuade företagen var till övervägande del verksamma inom, IT, IKT och tillverkning, se figur 3. Branschfördelningen var bredare och jämnare för enkätundersökningen, se figur 4. Enkäten hade 31 respondenter.

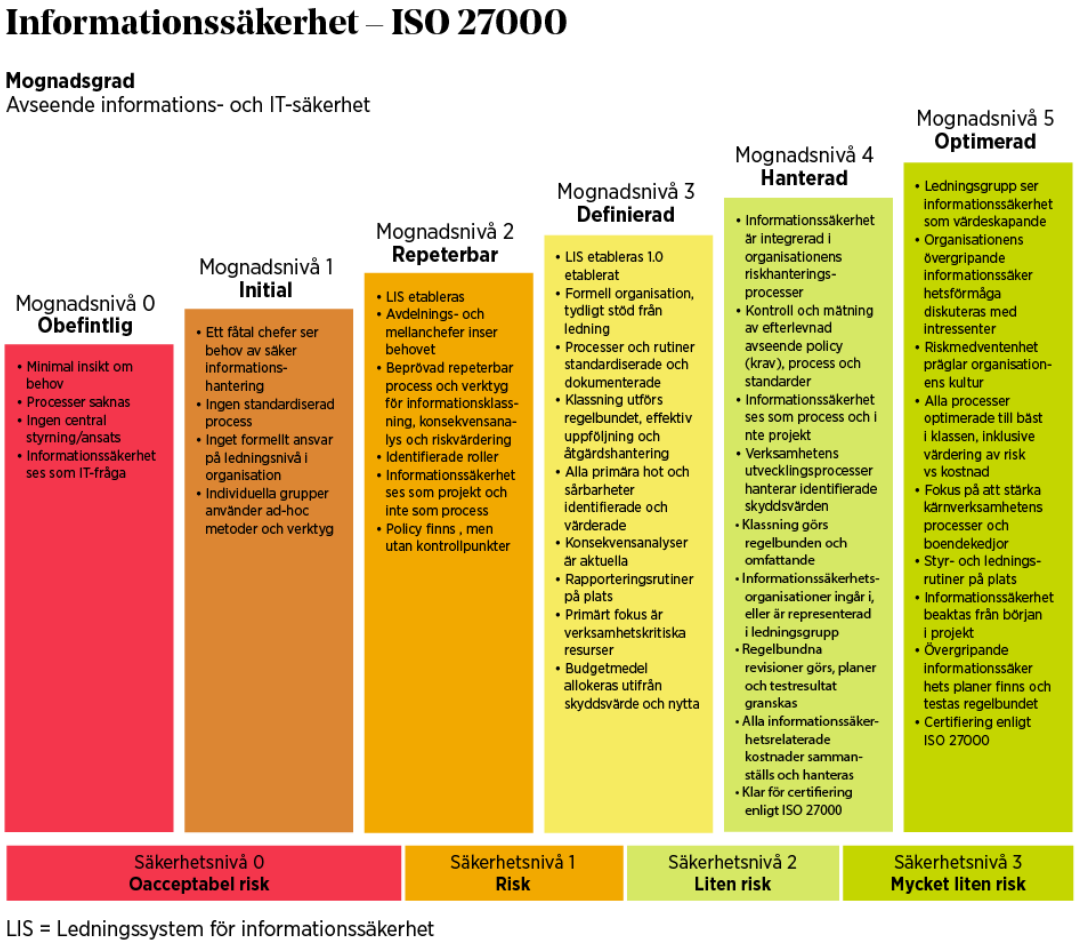
Djupintervjuerna gav ett mer detaljerat resultat än en webbenkäterna och har en större tyngd i reflektioner och rekommendationer än webbenkäterna. Samtliga företag har tillväxtambitioner men alla har inte internationella tillväxtambitioner.



Figur 3: Branschfördelning av alla intervjuade företag, där flertalet kommer från IT-verksamhet, informations- och kommunikationsteknik samt tillverkning.

4.1 Digitaliserings- och informationssäkerhetsmognad

Under kartläggningen identifierades ett behov av att kunna gruppera företagens mognad avseende informations- och cybersäkerhet. Hur de arbetar med dessa frågor är inte direkt kopplat till klassiska indelningar som branscher och storlek på företag utan snarare till andra faktorer såsom vilka kunder de arbetar mot, lagkrav och hur långt företaget kommit i sin egen digitalisering.

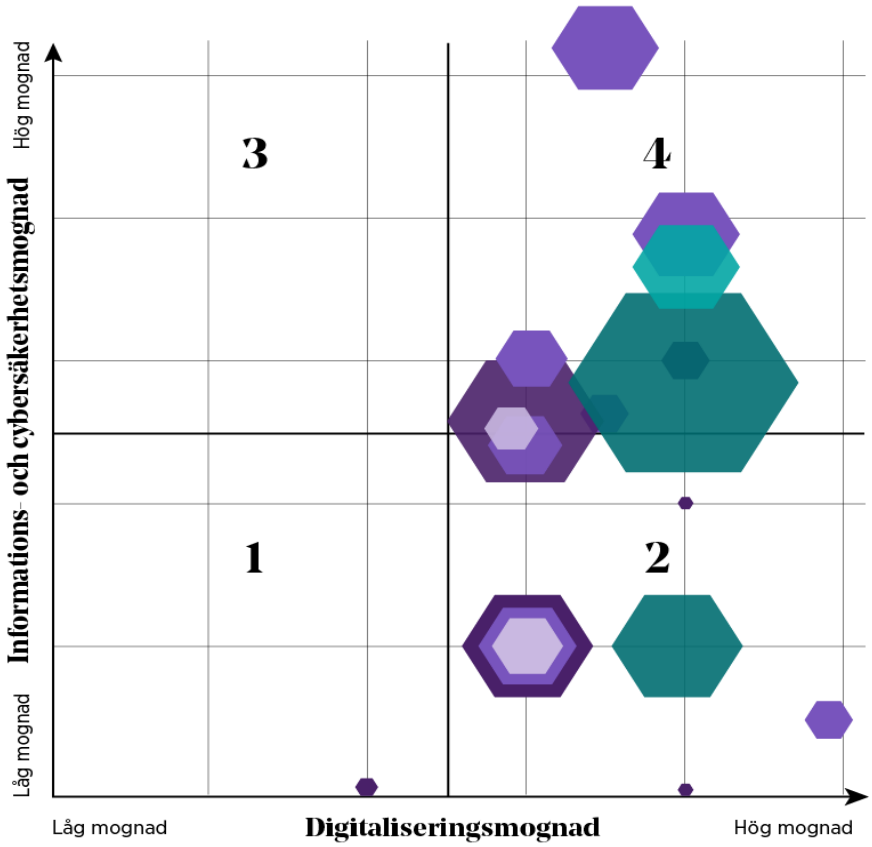


Figur 4: Uppnådd mognad av informations- och IT-säkerhet hos de bolag som har intervjuats.

4.2 Klassificeringsmatris

Samtliga företag som deltog i djupintervjuerna har utifrån svar skattats på en löpande skala över upplevd digital mognad och en löpande skala över upplevd mognad av informationssäkerhets- och cybersäkerhetsarbete i en klassificeringsmatris.

Matrisens kvadranter:



Klassificeringsmatris över upplevd digital mognad och upplevd mognad av informations- och cybersäkerhetsarbete.

Figur 5: Klassificeringsmatris, se vidare beskrivningar nedan.

1. Låg digital mognad, låg mognad av informations- och cybersäkerhetsarbete

Denna grupp som både har låg digital mognad och låg förståelse för hur man arbete med informations- och cybersäkerhetsfrågor hanteras, antas inte ha kommit långt i sitt arbete med digitalisering. Detta förutsätter dock att grundläggande funktioner finns på plats såsom digitaliserad lönehantering och att kommunikation sker via digitala media som e-post och IP-telefoni.

Denna grupp har inte frågor om informations- och cybersäkerhet på agendan. Om det skulle hända någonting så är åtgärderna reaktiva. Det finns inga processer och inget systematiskt arbete som stöd för organisationen att arbeta efter.

2. Hög digital mognad, låg mognad av informations- och cybersäkerhetsarbete

Denna grupp har hög digital mognad men saknar förståelse för de risker organisationen utsätts för om arbete inte hanteras strukturerat med informationssäkerhet. Gruppen

använder digitala verktyg och har merparten eller all information i digitala processer. Samtliga eller stora delar av kundrelationerna hanteras digitalt och sina huvudprocesser, där intäkter genereras, i digitala tjänster eller starkt kopplade till digitala lösningar.

Företag i denna grupp saknar förståelse för den påverkan som förlust av information kan ha och har inget systematiskt arbete för identifiering och skydd av sin information. Eventuella incidenter hanteras reaktivt.

Risken för att drabbas av allvarliga störningar i organisationen eller bli av med värdefulla data ökar desto större del av företagets processer som digitaliserats. Företag i denna kvadrant bör medvetandegöras om de risker de utsätter sig för och hur de kan arbeta proaktivt för att skydda sin information.

Intervju med tillväxtföretag inom utbildningsbranschen i grupp 2

Företaget är en startup i tydlig tillväxt med sju anställda. De behandlar stora mängder data om kunder och drar slutsatser från dessa. Företaget använder maskininlärning och Big Data för att transformera utbildningsbranschen. Deras huvudsakliga fokus är funktionalitet i sin produkt och marknadsandelar utifrån den fas man befinner sig i. Företaget har inte reflekterat över informations- och cyberrisker som en viktig del i verksamheten. Förtroendet för att tjänsteleverantörerna upprätthåller säkerhet är högt.

Hur bedömer du att kompetensnivån gällande digital transformation samt informations- och cybersäkerhet är hos personer i er ledning?
– Det är absolut något man tar hänsyn till, men frågan är inte prioriterad.

Vad är det viktigaste för er att ta hänsyn till vid val av system- och tjänsteleverantörer?
– Funktion är det viktigaste. Det får inte ta tid och får inte strula. Vi har all information i Amazon. Vi litar på Amazon kring säkerhetsaspekterna. Om vi hade tagit en mindre leverantör så hade säkerhetsfrågor varit viktigare.

I vilken utsträckning arbetar ni i nuläget strategiskt och medvetet för att dra affärsmässig nytta av ny digital teknik?
– Allt vi gör handlar om att använda digital teknik. Men fokus är inte att använda ny teknik, utan det handlar snarare hur man kan tillföra lärandet och det behöver inte vara just ny teknik. Men den blir viktig då det kan vara en förutsättning för att utveckla lärandet.

3. Låg digital mognad, hög mognad av informations- och cybersäkerhetsarbete

Denna grupp som har låg digital mognad och hög förståelse för hur arbeta med informations- och cybersäkerhetsfrågor hanteras, antas inte ha kommit långt i sitt arbete med digitalisering. Detta förutsätter dock att grundläggande funktioner finns på plats såsom digitaliserad lönehantering och att kommunikation sker via digitala media som e-post och IP-telefoni.

Företagen i denna grupp arbetar i hög grad systematiskt med informations- och cybersäkerhetsarbete. Riskerna företagen utsätter sig för är därmed låga utifrån ett informations- och cybersäkerhetsperspektiv.

4. Hög digital mognad, hög mognad av informations- och cybersäkerhetsarbete

Denna grupp har hög digital mognad och hög förståelse för hur arbete med informations- och cybersäkerhetsfrågor hanteras. Gruppen använder digitala verktyg och har merparten eller all information i digitala processer. Samtliga eller stora delar av kundrelationerna

hanteras digitalt och sina huvudprocesser, där intäkter genereras, i digitala tjänster eller starkt kopplade till digitala lösningar.

Företagen i denna grupp arbetar i hög grad systematiskt med informations- och cybersäkerhetsarbete. I denna grupp görs avvägningar mellan vilka digitala risker man utsätter sig för och hur skyddet i form av information- och cybersäkerhet ska anpassas i förhållande till riskerna.

Samtliga företag som arbetar med digitala processer bör sträva efter att befinna sig i denna kvadrant.

Intervju med tillväxtföretag inom hälso- och sjukvårdsbranschen i grupp 4

Företaget är ett offentligt publikt bolag med ca 50 anställda som har verksamhet inom test- och kvalitetssäkring kopplat till sjukvården. Företaget har ambitioner att växa, men inte internationellt. Företaget är certifierade enligt ISO 9001 (kvalitet) och ISO 27001 (informationssäkerhet) Ett resultat av detta är att de har ett strukturerat arbete med informations- och cybersäkerhetsfrågor.

Hur viktig är just säkerhetsaspekten vid val av system- och tjänsteleverantörer?
– Riskanalyser görs och ingår som aspekt i upphandling. Det är en viktig aspekt för oss.

Vad betyder informations- och cybersäkerhet för er, och i vilken utsträckning arbetar ni aktivt och systematiskt med dessa frågor?
– Vi jobbar systematisk med informationssäkerhet eftersom vi är certifierade. Viktigt med säkerheten, får inte bli hackade, inget får läcka ut, att informationen är korrekt samt avtalad tillgänglighet. Vi har informationssäkerhetspolicy och ansvariga roller utsedda.

I vilken utsträckning arbetar ni i nuläget strategiskt och medvetet för att dra affärsmässig nytta av ny digital teknik?
– Vi har Office 365, digitala system för tidrapportering, elektroniska fakturor och digitala verktyg för utveckling samt test och kvalitetssäkring.

4.2.1 Reflektioner

Djupintervjuerna genomfördes till stor del med företag inom IT-branschen. För att kunna skönja om resultaten är generella för olika branscher behövs ett utökat underlag av intervjuer från fler branscher.

De företag som identifierats i kvadranten som beskrivs under grupp 2, det vill säga hög digital mognad och låg mognad av informations- och cybersäkerhetsarbete, är de som är mest intressanta att studera eftersom de utsätter sig för stora risker där hela deras digitala affärsmodell hotas om de inte har tydligare fokus på ett systematiskt informations- och cybersäkerhetsarbete.

Exempelintervjuerna ovan visar på hur företag resonerar i sitt förhållande till informations- och cybersäkerhetsrisker. Företag i grupp 2 har kännedom om att dessa frågor är viktiga, men väljer ofta att lita på någon annan för att adressera riskerna. Företag i denna grupp ser risker, men tillåter sig att prioritera bort dessa till förmån för andra frågor som upplevs viktigare för bolagets fortsatta lönsamhet. Nyckeln till att få företag i grupp 2 att ta till sig frågor om informations- och cybersäkerhet är att göra det ”lätt att göra rätt”, det vill säga hitta enkla tekniska lösningar som tillåter frågor om informations- och cybersäkerhet att fungera smidigt i företaget utan att sätta hinder för fortsatt utveckling. Exemplet tidigare i grupp 4 visar på detta.

5 Tema 1: Digitala affärsmodeller och strategier

5.1 Företagens digitala utmaningar och risker

Analys av djupintervjuerna

Digitalisering är en strategiskt viktig konkurrensfördel för alla intervjuade branscher. Däremot finns skillnader i hur digital teknik utnyttjas strategiskt i affärsmodeller för de olika branscherna. Skillnaderna i digital mognad hos företagen speglas i värdet av digitaliseringen för företaget, vilket kan ligga på olika nivåer i digitaliseringens spektra.

IT-branschen utnyttjar ofta ny digital teknik för att effektivisera tjänster och/eller produkter åt kunder. Ständig teknisk innovation för effektivisering är nödvändig för att bibehålla konkurrensfördel. Hotell- och restaurangverksamhet utnyttjar även avancerad teknik för att kunna vara där kunderna är och underlätta för dem, exempelvis genom ”appar” i mobilen för bokning och rumsnyckelhantering.

Kulturella och kreativa näringar, informations- och kommunikationsteknik samt bygg- och tillverkningsbranschen fokuserar på strategisk digitalisering istället för på den interna verksamheten. Det kan innebära effektiva affärssystem, marknadsföring eller digital kommunikation för att tillgängliggöra information.

Affärsmodeller som är mest utsatta för risk är de som utnyttjar ny digital teknik men som inte hanterar information som faller under lagkrav. IT-verksamhet har stor press för att leverera funktionella, innovativa, tillgängliga och effektiva produkter och tjänster snabbt, vilket kan innebära att säkerheten prioriteras lägre.

Små tillväxtföretag är utsatta för ett flertal informationssäkerhetshot, exempelvis kan ett produktionsavbrott ge enorma ekonomiska konsekvenser om företaget drabbas av ransomeware på grund av avsaknad av virusskydd och de dessutom har undermålig säkerhetskopiering. De väljer i högre grad molntjänster vilket kan vara en risk om de inte upphandlas på ett korrekt sätt, exempel genom att informationen kommer i orätta händer. Breddföretagen har å andra sidan större organisatoriska utmaningar att hantera.

IT-företag som jobbar med digitalisering åt andra kunder uppger att man prioriterar rådgivning till kunder inom området istället för att jobba aktivt med den interna verksamheten.

Få små tillväxtbolag har IT-säkerhetsfokus i första hand vilket gör dem sårbara för ett flertal allvarliga hot. Dessa hot kan påverka verksamheten i olika grad, från merarbete, till allvarliga skador på varumärket. I värsta fall konkurs.

Några exempel på kända IT-incidenter:

- Bristande IT-kunskap medförde att miljontals känsliga vårduppgifter låg direkt åtkomliga på internet utan skydd.
- Ett serverrum som vattenfylldes medförde att hårddiskar inte kunde återskapas och därmed försvann all verksamhetsinformation.
- Ransomwareattacker som krypterade all verksamhetsinformation och trots att företaget betalade attackerarna fick de inte tillbaka informationen.
- Besviken, avskedad medarbetare raderade alla verksamhetsinformation och backuper. Informationen gick inte att återskapa.

5.1.1 Stor tillit till molntjänster

Många intervjuade företag anser att de inte upplever någon hotbild, att de inte har eftertraktad information eller kritisk mängd information. Företagen litar på att de molntjänster de anlitar hanterar säkerheten eller så är de för små för att prioritera informationssäkerhet. Många har uppfattningen att det inte är av betydelse, en konkurrensfördel, att jobba systematiskt med informationssäkerhet. En stor utmaning hos små tillväxtföretag är därför bristen på kunskap om olika digitala affärsrisker och hur de kan kopplas till företagets affärsvärde.

Idag är det enkelt för ett företag beställa IT-system och fylla dem med information utan att reflektera kring frågor om hur informationen hanteras av leverantören. Merparten av de intervjuade företagen litar fullt på leverantörerna att de tillhandahåller säkra och pålitliga tekniska lösningar och plattformar som de kan bygga vidare sina digitala processer och innovationer på.

Olika prisnivåer för molntjänster – basnivån täcker bara grundläggande säkerhet

I många fall är detta en bra situation för små tillväxtföretag, de får tekniska tjänster som gör informationen säkrare än om samma tekniska plattform skulle byggas upp från grunden med egen personal. Vad många företag missar är att molnleverantörer ofta har prisnivåer i sina erbjudanden, där basnivån endast erbjuder en grundläggande nivå av säkerhet. Rätt nivå av informationssäkerhet kostar och kommer inte att inkluderas i IT-system eller molnbaserade tjänster så länge inte kunderna kräver det och är beredda att betala för det eller att det finns lagkrav.

Svårt ha rätt och relevant egen kompetens i små företag

Informationssäkerhet är för de flesta små företagen en komplex fråga och svår att ta till sig på grund av dess omfattning. Det är även svårt för dem att ha relevant intern kompetens eftersom budget och tid ofta är begränsad. I den mån företagen arbetar med informationssäkerhet är det i huvudsak mot kund men inte lika systematiskt i den interna verksamheten.

Anne-Marie Eklund Löwinder om val av system och tjänsteleverantörer:

Vad ska man som ett litet och medelstort företag tänka på när man köper serverkapacitet hos en molnleverantör?
– Molntjänster är hur bra som helst – när det fungerar. Men det är inte så enkelt som att bara slå på en kran och det fungerar. Ta professionell hjälp. Om det bara handlar om serverkapacitet för lagring är det kanske enkelt. Informationsskydd är centralt, och kryptering är svaret på frågan. Nyckeln ska man ha själv. Och ta egna backuper. Att ha all data på ett ställe är alltid en risk, även i molnet. Ställ krav på möjlighet till regelbundna datadumpar, se till att leverantören har ett patchschema för uppdateringar av OS med mera och att man har incidenthantering/-rapportering. Tänk också på att det inte är ”allt eller inget” utan att du kan välja att lägga delar av verksamheten i molnet.

5.2 Etablera rätt nivå av informationssäkerhet

Alla organisationer måste etablera och vidmakthålla rätt nivå av informationssäkerhet. Om nivån är för låg kan konsekvensen bli att företagen utsätter sig för stora risker som kan påverka både varumärket och ekonomin. Små företag har i regel mycket liten förståelse för området vilket gör att de är extra utsatta för dessa risker. Å andra sidan kan nivån också vara för hög hos vissa företag. Då kan konsekvensen bli att kostnader för tekniska och administrativa åtgärder blir höga eller att det blir svårt att arbeta. Samt sänkt säkerhet när kreativa medarbetare hittar andra sätt att arbeta på, exempelvis att de skickar känslig information via e-post för att kunna arbeta hemma.

För att skapa rätt nivå bör företagets ledning, **enligt standarden ISO/IEC 27001**, beakta bland annat följande;

- Identifiera lagkrav
- Identifiera krav från intressenter, exempelvis kunder och ägare
- Genomföra riskanalyser
- Klassificera informationen utifrån dess skyddsvärde
- Tillsätta en informationssäkerhetsorganisation
- Ta fram tekniska och administrativa skyddsåtgärder för informationen
- Utbilda personalen så att de vet hur de ska agera och varför
- Skapa ledningens engagemang och insyn via en årlig genomgång
- Återkommande arbeta systematiskt med ovanstående, såsom standarden ISO/IEC 27001 rekommenderar

5.3 Reflektioner

5.3.1 Behov av systematiskt arbete med informations- och cybersäkerhet

Systematiskt informationssäkerhetsarbete bör vara en förutsättning för en hållbar och säker digitalisering. Aktiviteter som *informationsklassning*, *riskanalys* och *hantering av incidenter* minskar risken för problem såsom dataintrång och dataförlust och att drabbas av höga sanktionsavgifter under GDPR.

Senare kapitel i rapporten fokuserar på vikten av ledningens engagemang för ett långsiktigt hållbart arbete med digitalisering. Små tillväxtföretag har ofta ett större risktagande än etablerade företag när det gäller aktiviteter som inte direkt bidrar till att bygga produktens/tjänstens värde. Att systematiskt arbeta med risker gör att det blir möjligt att identifiera risker som under en längre period utgör ett hot för företaget. Ett systematiskt arbete med informationssäkerhet och digitala affärsrisker gör att cyberhot och förlust av information blir tydligt även för mindre företag eftersom sådana händelser kan påverka företagets långsiktiga plan att lyckas.

Särskilt företag med hög digitaliseringsgrad och låg mognad inom informations- och cybersäkerhetsarbete kan behöva medvetandegöras om riskerna de utsätter sig för.

5.3.2 Påverkan på varumärket

En faktor till att förståelsen för ett systematiskt informationssäkerhetsarbete är låg kan vara att i de fall företag har drabbats av cyberincidenter har påverkan på svenska företags varumärken inte påverkats nämnvärt fram till nu. Ett exempel på det är 1177-händelsen där en stor mängd inspelade samtal till 1177 Vårdguiden hade legat oskyddade på internet (SLL:s svar till Datainspektionen 2019). Även om händelsen fick stora rubriker skadades i

detta fall inte förtroendet för Vårdguiden i någon större utsträckning. Den aktör längst ned i outsourcingkedjan som var orsaken till den dåliga säkerheten var ett mindre företag vars varumärke har påverkats kraftigt på grund av dålig publicitet samt en pågående tillsyn av Datainspektionen. För andra företag kan påverkan på varumärket vara betydligt större.

Om tillväxtföretag har en affärsmodell som är beroende av ett fåtal viktiga kunder eller befinner sig på en marknad där det är enkelt att växla kunder är frågor kring cyberrisker och informationssäkerhet ytterst viktiga för företagets långsiktiga fortlevnad. Även små tillväxtföretag måste ställa sig frågan vad som skulle ske vid en större incident som företaget själv orsakar eller är delaktig till.

Trenden går mot en förändring i samhället. Kunderna förväntar sig att företagen hanterar information på ett säkert sätt. Regelverk såsom GDPR och kommande ePrivacy förordning ställer krav även på små tillväxtföretags verksamhet. Det kan inom kort komma att förändra vad som är accepterat och mycket tydligare påverka förtroendet för företagens varumärke vid incidenter och vad som får drabba deras kunder.

Anne-Marie Eklund Löwinder, CISO på Internetstiftelsen, om systematiskt informationssäkerhetsarbete

Anne-Marie är en av pionjärerna inom internet i Sverige och en av de sju experter på internetsäkerhet som är Trusted Community Representative och Crypto Officer, det vill säga har nycklar till en av de två av ICANN:s år 2010 upprättade datacentraler, som upprätthåller identifieringssäkerhet för Internets adressregister DNS i Internets rotzon. 2013 blev Anne-Marie Eklund Löwinder den förste svensken att bli invald i Internet Hall of Fame. Hon sitter i styrelsen för Council of European National Top Level Domain Registries, Institutet för rättsinformatik och Swedish Network Users' Society.

Vilka fördelar kan små och medelstora företag få genom att arbeta systematiskt med informationssäkerhet?
– Det blir allt viktigare att ha tillgång till information för att företaget ska fungera utan störningar och avbrott. Fördelen med att arbeta systematiskt är att man har kontroll och arbetar med ständiga förbättringar. MSB har gett ut rekommendationer för företag med upp till 10 anställda om hur de kan arbeta med informationssäkerhet. Det är en bra början att läsa och ta till sig det som står där (MSB, 2019a).

Informationssäkerhet och cybersäkerhet är viktigt, trots det är det många som inte prioriterar frågan. Varför tror du att det är så?
– Även om informationssäkerhet är viktigt är det brist på kompetens och resurser. Det ligger inte riktigt inom kärnverksamheten för många verksamheter idag. Men i en värld där 85 procent av verksamheters tillgångar är digital så borde det inte vara någon överraskning att kundernas, ägarnas och andras välvilja står i direkt korrelation till hur man hanterar information på ett säkert sätt.

Vilka möjligheter öppnas upp för företag som jobbar förebyggande och aktivt med sin IT-säkerhet?
– Ett riskbaserat, systematiskt informationssäkerhetsarbete, med uppföljning – gör att organisationer effektivt kan nyttja den egna kompetensen. Frånvaron ger en oacceptabel sårbarhet. Säkerhet påstår jag, gör företag mer framgångsrika och intressanta om de utnyttjar investeringen till att förädla affärsmodeller, erbjudanden och prissättning. En fråga för verksamhetens strategiska ledning alltså. Det går inte att överlåta dessa frågor till IT-avdelningen. Det är som att ha bocken som trädgårdsmästare.

Samhället är idag strikt reglerat på alla plan, varför finns det så få krav på små och medelstora företag hur man jobbar med IT och Cybersäkerhet?
– Vi ser idag en "Regelexplosion" som man kan tolka som en vilja att komma till rätta med brister. Det kanske tyder på en ökad medvetenhet bland de styrande och de styrda. GDPR 2018. NIS-direktivet 2018. Nya regler sätter fokus på informationssäkerhet inom viktiga samhällssektorer som energi, transport med flera. Vi utgår dock ofta från att problemet är illvilliga aktörer trots att nästan alla stora läckor av information har orsakats av den egna verksamhetens oförmåga att göra rätt. Vi skjuter oss själva i foten. Jag tycker väl ändå att det ställs en hel del krav, men vi har en ansvarsprincip i Sverige, som innebär att det är verksamheten som måste se till att skydda sina viktigaste tillgångar. Det är vi vana att göra i den fysiska världen, men på något sätt har IT flugit under radarn för många företagsledningar så här långt. Det funkar inte längre.

6 Tema 2. Utbud inom informations- och cybersäkerhet

6.1 Den offentliga styrningen av samhällets informations- och cybersäkerhet

2018 presenterade regeringen en nationell strategi för samhällets informations- och cybersäkerhet (Regeringen 2018b). Strategin ska bidra till att skapa långsiktiga förutsättningar för samhällets aktörer att arbeta effektivt med informations- och cybersäkerhet samt att höja medvetenheten och kunskapen i hela samhället. Strategin omfattar statliga myndigheter, kommuner och regioner, företag, organisationer och privatpersoner. Av strategin framgår att ett strukturerat och riskbaserat arbete med informations- och cybersäkerhet är en viktig förutsättning för svensk tillväxt och konkurrenskraft, och en nödvändighet för att näringslivet ska kunna utveckla och tillhandahålla konkurrenskraftiga varor och tjänster.

Samma år gav regeringen i uppdrag till Myndigheten för samhällsskydd och beredskap, MSB, att öka allmänhetens samt små och medelstora företags kunskap om informationssäkerhet, inklusive frågor om id-stölder (Regeringen 2018c). Uppdraget redovisades i januari 2019 med en redogörelse över insatser som genomförts för att stärka kompetensen och förmågan att höja cybersäkerheten, bland annat kampanjen Tänk säkert – skydda din viktigaste information! (MSB med flera, 2019).

Regeringen har vidare lämnat en rad uppdrag till flertalet myndigheter inom ramen för den nationella strategin bland annat till MSB i samverkan med Försvarets radioanstalt, Försvarets materielverk, Försvarsmakten, Post- och telestyrelsen, Polismyndigheten och Säkerhetspolisen att ta fram en samlad informations- och cybersäkerhetsplan (Regeringen 2018d) och till Tillväxtverket att utveckla och genomföra ett program för att öka kunskapen hos småföretags ledningar och styrelser (se ovan).

I juni 2019 fick Tillväxtverket ytterligare ett uppdrag att kartlägga förutsättningarna för att öka små och medelstora företags förmåga att använda data strategiskt (Regeringen 2019a). Uppdraget ska dra nytta av synergieffekter av tidigare uppdrag som pågår.

6.1.1 Myndigheten för samhällsskydd och beredskap, MSB

Tänk säkert-kampanjen

Oktober är informationssäkerhetsmånaden, ett EU-initiativ som syftar till att öka medvetenheten om vikten av informationssäkerhet i hela Europa. I Sverige finns ett samarbete mellan MSB, myndigheten för samhällsskydd och beredskap, Polisens nationella bedrägericenter och flera andra organisationer, bl. a Verksamt.se för att höja baskunskaperna om informationssäkerhet hos mindre företag.

Tänk säkert-kampanjen har en hemsida: DinSäkerhet.se som riktar sig både till allmänhet och företag, särskilt mikroföretag, och ger olika tips om vad man själv kan göra för att skydda sig mot brott och skydda sin information.

Nationellt cybersäkerhetscenter

Regeringen lämnade september 2019 ett uppdrag åt Försvarets radioanstalt, Försvarsmakten, MSB och Säkerhetspolisen att tillsammans vidta förberedande åtgärder och lämna förslag för att ett nationellt cybersäkerhetscenter ska kunna inrättas under 2020 (Regeringen 2019b). Det nationella cybersäkerhetscentret ska stärka Sveriges

samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot mot Sverige och minska cybersårbarheterna. Vidare ska centret ge ett utvecklat och samordnat stöd om hur olika aktörer i privat och offentlig sektor kan skydda sig mot cyberattacker där en central del kan vara gemensamma analyser och lägesbilder om hot, sårbarheter och risker. Centret ska också kunna understödja Regeringskansliet i frågor kring cybersäkerhet.

Analys av möjligheterna att stödja kompetensförsörjning

MSB kommer att analysera möjligheterna att stödja kompetensförsörjning inom informations- och cybersäkerhetsområdet. MSB har även till ansvar att utreda vilka åtgärder som skulle krävas. Arbetet koordineras med redan pågående aktiviteter som genomförs av andra aktörer. Åtgärden genomförs tillsammans med relevanta aktörer i samhället under 2019–2020 (*MSB 2019*).

6.2 Utbud av olika erbjudanden inom informations-, cyber- och IT-säkerhet

Det finns ett stort utbud av tjänster på marknaden inom informations- och cybersäkerhet som riktar sig till företag av olika storlek. Om ett företag har beslutat sig för att arbeta med sina digitala affärsrisker på ett strukturerat sätt finns både offentliga och privata alternativ tillgängliga.

6.2.1 Certifieringar och standarder

SSF Cybersäkerhet Basnivå (Stöldskyddsföreningen, 2019a)

SSF Cybersäkerhet Basnivå hjälper organisationen att vidta ett antal lämpliga och relevanta säkerhetsåtgärder vilka leder till en bra IT-säkerhet. SSF Cybersäkerhet Basnivå ska fungera som ett första steg i organisationers arbete att höja förmågan att möta risker kopplat till informationshantering och därmed även bidra till att stärka samhällets samlade informationssäkerhetsarbete. Certifieringen riktar sig främst till mindre företag

ISO/IEC 27001:2017 Ledningssystem för informationssäkerhet.

Standard SS-ISO/IEC 27001:2017 fastställer krav som en organisation behöver uppfylla när det gäller ledningssystem för informationssäkerhet (LIS), bl.a. krav för delmomenten

- upprättande
- införande
- underhåll
- ständigt förbättringsarbete

Standarden innehåller även krav för bedömning och behandling av informationssäkerhetsrisker. Den kan vidare användas för bedömning av en organisations förmåga att uppfylla informationssäkerhetskrav, såväl internt som av externa parter.

ISO/IEC 27701:2019 Privacy Information Management System

(Komplettering till ISO 27001 för dataskydd, engelska)

NIST Cybersecurity Framework (NIST, 2019).

NIST är till skillnad från ISO 27001 ett gratis ramverk. NIST är ett amerikanskt ramverk och en lightversion av ISO 27001.

NIST Privacy Framework (NIST DRAFT 2019)

NIST Privacy är ett verktyg för organisationer att bättre kunna identifiera, styra, kommunicera och bedöma integritetsrisker.

6.2.2 Rådgivning, vägledningar och självtester

- Informationssäkerhet för små företag – Rekommendationer för dig som driver eget företag med upp till 10 anställda (MSB, 2019a).
- Stöldskyddsföreningen har tillsammans med MSB tagit fram en norm för IT - säkerhet för små och medelstora företag och organisationer (Stöldskyddsföreningen, 2019b) Principerna är framtagna med stöd av Polisen och flera branschorganisationer, bland annat Svenskt Näringsliv och Svensk Handel med en målsättning att höja samhällets samlade informationssäkerhet. Här finns även ett enkelt test där man kan testa sin IT-säkerhet genom att svara på frågor inom olika områden.
- Försäkringsförmedlaren Aon har ett verktyg för självtest, Cyber Risk Diagnostic Tool (Aon, 2019). Verktyget identifierar de viktigaste interna och externa faktorer som kan påverka ett företags sårbarhet.
- Center for Internet Security, CIS, har tagit fram CIS Controls som är en prioriterad lista med handlingar för att forma ett så kallat ”defense in depth” för de vanligaste attackerna mot system och nätverk (CIS, 2019).
- FINRA Cybersecurity Checklist (Checklist) FINRA är en amerikansk statligt auktoriserad ideell organisation som övervakar amerikanska mäklare-återförsäljare.
- Grundläggande IT-säkerhetsåtgärder, förstahandsutgåva (MSB, 2019b) Fastställd utgåva planerad till hösten 2019.
- DinSäkerhet.se (DinSäkerhet, 2019a) som drivs av MSB har också en egen spellista (DinSäkerhet, 2019b) på YouTube där samtliga av webbplatsens filmer kring informationssäkerhet finns.

6.2.3 Konsultföretag

Det finns flera företag som erbjuder specialiserade tjänster inom allt från riskhantering, revisioner och rådgivning till teknisk design och införande av IT-säkerhetslösningar. Till dessa tjänster kopplas ofta erbjudande om utbildning. Generellt erbjuder företagen dessa typer av tjänster:

Tjänster inom säker digital transformation och strategi

Tjänster för digital transformation driven ur ett informationssäkerhetsperspektiv, ofta kopplat till effektivt utnyttjande av molntjänster. Hantering av AI, ny teknologi med mera.

Tjänster inom informationssäkerhet

Tjänster med specialistkompetens inom informationssäkerhet som stöttar kunder i arbetet med att minimera risker kopplade till säkerhet samt att efterleva regelverk. Dessa tjänster inkluderar:

- **Risk och sårbarhetsanalys och kontinuitetsplaner**
  Hjälper företag med genomförande av risk- och sårbarhetsanalyser
- **Införande av Ledningssystem för informationssäkerhet, LIS**

Hur företag ska arbeta och föra in ett ledningssystem för systematiskt informationssäkerhetsarbete (ISO 27001)

- **Revisioner av organisationer, efterlevnad och certifiering**
  Granskningar och revisioner av att organisationer uppfyller sina egna krav eller krav man certifierat sig mot
- **Krishantering vid cyberattacker**
  Hjälper organisationer att praktiskt öva inför större incidenter
- **Rådgivning kring lagar och regleringar som säkerhetsskyddslagen, NIS-lagen, GDPR med flera**
- Rådgivning så att organisationer når upp till krav som ställs på dem enligt relevanta regelverk inom området

Tjänster inom dataskydd och GDPR

- **Dataskyddsombud som tjänst**
  Tillhandahåller tjänst som externt dataskyddsombud
- **Dataskyddsorganisation som tjänst**
  Tillhandahåller tjänst för extern dataskyddsorganisation inklusive dataskyddsombud
- **GDPR införande**
  Bistår med program för införande av processer och rutiner för dataskydd i organisationer så att de efterlever regelverket

Tjänster inom övervakning av infrastruktur

Företagen tillhandahåller en övervakningscentral ofta kallat Security Operations Center, SOC, där operatörerna övervakar och analyserar nätverkstrafik och loggar i syfte att stoppa angripare och skadlig kod hos deras kunder, dygnet runt, året om.

- **Intrusion Detection**
  Detektering av intrång och aktivt bistånd om så sker
- **SIEM & Log Management**
  Övervakning av loggar och analyser av dessa
  Endpoint Protection
  Skydd av datorer via olika metodiker såsom analys i realtid och identifiering när kod beter sig onormalt på klienter och servrar
- **Threat Intelligence**
  Övervakning av publika och privata källor samt Darknets i syfte att identifiera olika sorters hot och aktivitet.

Tjänster inom teknisk IT-säkerhet

Tjänster som identifierar säkerhetsbrister i nätverk, system och applikationer. Även hantering och utredning av kritiska incidenter ingår.

- **Tekniska säkerhetsgranskningar**
  Tjänster för att aktivt bryta sig in i uppdragsgivares tekniska miljöer för att hitta brister i den tekniska miljön
- **IT-brottsutredningar**
  Tekniker och processer för att säkra bevis som är rättsligt giltiga vid en rättslig prövning
- **Social engineering**
  Identifiering av tekniker för att manipulera människor så att de lämnar ifrån sig konfidentiell information

- **Incidenthantering**
  Bistånd vid aktiva incidenter för återställning av normal drift och förbättring av processer
- **Behörighetskontroller**
  Bistånd vid säkerställandet av att ett företag har korrekta behörigheter för de roller som personal och kunder har

6.3 Erbjudanden företagsfrämjare

Flertalet företagsfrämjare[1] har erbjudit eller erbjuder någon form av stöd, information och rådgivning relaterat till informations- och cybersäkerhet. Några har tagit in externa föreläsare som är experter i ämnet för att informera under frukostseminarier och liknande. Andra informerar ibland om informationssäkerhet i deras nyhetsbrev och på webben. Genomgående för alla är att de har haft omfattande information om GDPR.

För vissa är informationssäkerhet en oerhört viktig fråga och för andra beror det på rådgivarens erfarenhet och mognad att diskutera ämnet. Ingen har rätt kompetens internt och majoriteten anser att de själva behöver kompetens inom området innan de kan börja ställa frågor till företagen. Eftersom informations- och cybersäkerhet inte ingår i ordinarie rådgivning, eller inte ens i rådgivningen kring digitalisering för små och medelstora företag, behöver de själva förstå för att kunna hjälpa företagen.

6.3.1 Mer kan göras om efterfrågan finns

När det gäller företagens kompetens och sårbarhet tycker de flesta att det finns stor okunskap i ledningen för digitaliseringsfrågor. Säkerhetsfrågor och digitalisering ligger långt bort i de flesta ledningarna. Genom att de är inte är införstådda i informationssäkerhet och dess vikt för företaget blir de sårbara. Några tror att när företagen väl börjat digitalisera kan säkerhetsfrågor aktualiseras men även om företag förstår att det kan finnas risker vet de nog inte hur de ska skydda sig. Att företag är mer fokuserade på hinder och möjligheter med deras affärsidé och att skydda idéer, varumärken och patent.

De flesta får inte frågor inom området och det är inte heller ett krav idag att företagen har ett informationssäkerhetsarbete. Några vill vara mer proaktiva men vill också veta om behovet finns. Då skulle de kunna göra mer inom informationssäkerhetsområdet om tillräckligt många efterfrågar det.

6.4 Cyberförsäkringar

IT-utvecklingen innebär helt nya riskexponeringar som inte omfattas av traditionella egendoms- och ansvarsförsäkringar. Enligt rapporten Allianz Risk Barometer är avbrott i verksamheten, inklusive störning i leveranskedjan det största hotet för företag för sjunde året i rad. För första gången ansluter sig cyberincidenter till toppen av rankingen. Den genomsnittliga försäkrade förlusten från en cyberincident är enligt rapporten drygt 2 miljoner euro jämfört med nästan 1,5 miljoner euro vid en brand eller explosion. De svarande rankar cyberincidenter som det de fruktar mest, med tanke på att många företags primära tillgångar är just data, serviceplattformar eller kund- och/eller leverantörsregister.

[1] Baserat på 7 intervjuer av företagsfrämjare (bland annat Almi, Nyföretagarcentrum och Business Sweden)

World Economic Forum (The Global Risks Report 2019) beskriver cyberrisk som en av de mest väsentliga samhällsriskerna vid sidan av klimatrisker och naturskador. Sannolikheten för att angrepp inträffar har ökat och ett antal omfattande globala angrepp med stora informationsförluster och ekonomisk påverkan har inneburit att företag och organisationer betraktar denna risk som ökande.

Erbjudanden om teknisk support, rekonstruktion och ersättning

Flertalet försäkringsbolag i Sverige erbjuder så kallade cyberförsäkringar. I försäkringarna ingår oftast bland annat; dygnet runt teknisk support av IT-experter för att stoppa attacken och återställa data och IT-system, ersättning vid avbrott och för kostnader att rekonstruera och återställa data och programvara, ersättning vid ekonomisk förlust i samband med dataintrång, ersättning vid skada som drabbar tredje man, hjälp med juridisk rådgivning vid skadeståndsanspråk, PR-kostnader och hjälp med mediahantering och ersättning för kostnader för att underrätta kunder och andra berörda. Premierna på den svenska marknaden ligger i storleksordningen 0,5–1 procent av försäkringsbeloppet.

Många små tillväxtföretag har ofta en affärsidé som har stora digitala informationsmängder. Snabb och effektiv respons vid IT-incidenter är mycket viktigt för att inte förlora kundernas förtroende så denna ty av hjälp kan, tillsammans med företagens förberedande arbete med riskanalyser, bli mycket viktig. Samt att det finns strategier för att hantera kriser och större incidenter.

6.4.1 Cyberförsäkringar relativt okänt hos små tillväxtföretag

En cyberförsäkring kan aldrig ersätta en god riskhantering i en verksamhet. Ofta krävs att en organisation som vill teckna cyberförsäkring kan visa försäkringsbolaget att företaget bedriver ett systematiskt informationssäkerhetsarbete. Att teckna en försäkring utgör därför ofta ett stöd för verksamheten i arbetet med att förebygga och hantera risker. I kartläggningen framgick att de intervjuade företagen inte kände till att cyberförsäkringar existerar.

Relativt svalt intresse från småföretagen – rätt så ny produkt

En rundringning hos försäkringsmäklare och försäkringsbolag som erbjuder cyberförsäkringar visar att intresset för cyberförsäkringar fortfarande är ganska svalt. En försäkringsgivare gissade att det var under 5 % av småföretagen hos dem som hade en cyberförsäkring.

Majoriteten av försäkringsgivarna erbjuder cyberförsäkring som tillägg, endast ett företag erbjuder det i grundansvarsförsäkringen. Ett par försäkringsgivare har erbjudit cyberförsäkring i 2–3 år medan det för de flesta är en relativt ny produkt. Det är främst stora företag, med riskmedvetenhet och insikt om att en cyberförsäkring kan kapa toppen av kostnaderna för cyberskador, som tecknar denna typ av försäkring. Uppfattningen är att de små företagen tror att det inte händer dem eller att de inte har information som någon vill åt. De branscher där det är vanligast med cyberförsäkring är tekniska konsulter, vården och IT-drift leverantörer.

6.5 Reflektioner

Det finns ett stort utbud av aktörer som tillhandahåller kunskap och metoder för informationssäkerhet, speciellt myndighetsaktörer har tillgänglig information för olika målgrupper. Det är svårt att veta om informationen når de tilltänkta användarna. Den mest sedda filmen på MSB:s hemsida kring informationssäkerhet har strax över 17 000 visningar.

Uppfattningen är att små tillväxtföretag gärna tar hjälp av konsulter inom området när behov har identifierats.

Införandet av ett ledningssystem för informationssäkerhet är ofta en investering som kan ta lång tid för en organisation. Att anlita konsulter för ett införande blir en stor investering som inte prioriteras av små tillväxtföretag. Detta faktum syns tydligt i de intervjuer som genomförts i studien.

Företagsfrämjare har en stor möjlighet att hjälpa små tillväxtföretag med deras behov av kompetens inom informations- och cybersäkerhet genom att exempelvis:

- Ta fram checklistor, frågebatterier och liknande om informations- och cybersäkerhet och digitala risker vid kontakt och rådgivning.
- Synliggöra cyberförsäkringar tillsammans med försäkringsbolagen
- Vara språkrör för tillväxtföretagen och lösa gemensamma frågor
- Upphandla konsulter som specialiserar sig på tillväxtföretagens förutsättningar

Företagsfrämjare kan också i större utsträckning ta hjälp av befintliga aktörer och konsulter för att bygga in informationssäkerhet i sina egna processer. I de intervjuer som genomförts har ett utbildningsbehov identifierats, både för att stärka företagsfrämjarna i deras interna arbete, och i deras roll som företagsfrämjare.

Insikten om att cyberförsäkringar finns och vilket stöd dessa kan ge var okänt för samtliga intervjuade företag i studien. Om kännedom skulle öka bland tillväxtföretagen skulle konsekvenserna vid större IT-incidenter sannolikt kunna minskas avsevärt. Det finns dessvärre ingen tillgänglig statistik som entydigt visar värdet av denna försäkringstyp. Det är dock tydligt att med den ökande digitaliseringen blir cyberförsäkringar en viktigare del i tillväxtföretagens hantering av risker.

Anne-Marie Eklund Löwinder utbud inom informations- och cybersäkerhet

Tycker du samhället/staten hjälper små och medelstora företag tillräckligt? Om inte vad mer skulle man kunna göra för dem?
Frågan är splittrad på många olika myndigheter, jag tror ändå att man försöker hjälpa till. MSB publicerar rekommendationer, Stöldskyddsföreningen erbjuder utbildning och certifiering, verksamt.se har information (Verksamt.se, 2019). Vi på Internetstiftelsen bidrar med internetkunskap.se (Internetstiftelsen, 2019). Så, ja, jag tycker nog att hjälp finns. Svårigheten är att nå ut och att få företagen att lägga tid och resurser på frågan.

7 Tema 3. Lagstiftning och juridik

De affärsjuridiska utmaningarna tillväxtföretagen främst står inför är avtalsfrågor; affärsavtal, anställningsavtal och sekretessavtal. GDPR har varit eller är en utmaning för de flesta. De som vill växa internationellt ser att de behöver hantera många juridiska frågor, vilket är en begränsning för att ta steget till en internationell marknad.

De flesta har tillgång till affärsjuridiskt stöd, antingen via branschförbund, företagsfrämjare, tidigare anlitad jurist eller på rekommendation.

7.1 Lagstiftningens utmaning i den exponentiella teknikutvecklingen

Den snabba teknikutvecklingen medför att lagstiftningen hamnar på efterkälken. Människors beteenden förändras också i takt med utvecklingen och konsumtion sker inte längre endast sker i fysiska butiker på den lokala marknaden. Den sker även från andra länder och helst genom ett knapptryck via mobilen, surfplattan eller datorn. Ständig uppkoppling till sociala medier där personuppgifter sprids allt mer ökar risken för exempelvis identitetsstölder, bedrägerier, integritetskränkande fotografering och avlyssning. Istället diskuteras allt fler frågor om etik och moral som ett sätt att hantera rätt och fel inom oreglerade områden, inte minst inom AI.

Temat relationen mellan juridik, etik och teknik diskuteras flitigt både i forskarvärlden och i media. AI, Big data, IoT och algoritmer får en allt större betydelse på allt fler områden. Relationen mellan juridiken och tekniken är sedan länge uppmärksammad och behandlad. Idag är fokus mer på den etiska aspekten.

Det finns etiska uppförandekoder utformade för forskare och användare inom data och informationssystem, exempelvis ACM Code of Ethics and Professional Conduct (ACM, 2019). Uppförandekoden består av sju generella etiska principer; 1) bidra till samhället och det mänskliga välbefinnandet 2) undvik att göra skada 3) var ärlig och pålitlig 4) var rättvis och undvik diskriminering 4) respektera arbete som lagts ner på att producera nya idéer 5) innovationer 6) kreativt arbete och 7) föremål för datoranvändning, respektera integritet samt hedra konfidentialitet.

7.1.1 Sandlådor och stresstester för innovation och utveckling

I en artikel från ComputerSweden, 2019 anser Cecilia Magnusson Sjöberg, professor i rättsinformatik, att juridiken bör tas med från början i digitaliseringsprojekt så att den blir ett stöd istället för ett hinder. Juridiken behöver finnas med när system upphandlas, utvecklas och designas eftersom kostnaderna annars blir högre om juridik kommer senare i processen. Hon förespråkar också juridiska labb eller policylabb där befintlig lagstiftning kan prova sig fram. – Där skulle man i stället vilja se att myndigheter som Datainspektionen och Myndigheten för samhällsskydd och beredskap kunde få gå in och se till att testverksamhet kan ske legalt så att vi kan hitta konkreta modeller där det är tillåtet att utväxla data. EU arbetar mycket med externa rådgivande kommittéer och det är också en modell som Cecilia Magnusson Sjöberg tycker Sverige borde använda.

Den engelska motsvarigheten till Datainspektionen, ICO, startade i somras en testverksamhet som de kallar ”Data Protection Sandbox” (ICO, 2019). Sandlådan är utformad för att stötta exempelvis tillväxtföretag med dataskyddsfrågor när de utvecklar innovativa produkter och tjänster. Syftet är att hjälpa företagen att se till att risker förknippade med projektens användning av personuppgifter minskas. De utvalda

deltagarna täcker ett antal sektorer, bland annat hälsa, brottslighet, bostäder och artificiell intelligens.

Det finns dock risker med att testa sig fram vid utveckling av ny teknik. En gymnasieskola i Skellefteå fick exempelvis sanktioner på 200 000 kr genom ett försök med ansiktsigenkänning då de enligt tillsynsmyndigheten överträtt bestämmelser i GDPR. (Datainspektionen 2019)

Ett annat sätt att testa sina system under trovärdiga former är den testbädd som forskningsinstitutet RISE Cyber Range i Kista nyligen öppnat för att bidra till Sveriges cybersäkerhet (RISE Stresstest). Här får företag och organisationer en fysisk plats för att träna och utbilda medarbetare men också bygga en virtuell miljö som är helt kontrollerad, vilket i slutändan skapar stabila och säkra IT-system.

7.2 Lagar och regler som styr arbetet med informationssäkerhet

GDPR är det första regelverket som tydligt ställer krav på alla organisationers informationssäkerhet då skyddet av personuppgifter kräver ett systematiskt informationssäkerhetsarbete. Ett av syftena med GDPR var att få en gemensam lagstiftning beträffande behandling av personuppgifter inom EU och för att stärka den personliga integriteten. Trots att GDPR i första hand reglerar behandlingen av personuppgifter är åtgärder för dessa även tillämpbara för övriga information inom företaget.

Ett annat regelverk som kan styra arbetet med informationssäkerhet för små tillväxtföretag som även är kopplat till GDPR är kamerabevakningslagen. Privat verksamhet, som inte utför en uppgift av allmänt intresse, behöver inte längre tillstånd för att kamerabevaka. Istället anses GDPRs regler vara tillräckliga för att garantera att behandlingen av personuppgifter inte kränker enskildas personliga integritet. Företag som ska kamerabevaka måste göra en bedömning av varför de vill använda kamerabevakning och koppla det till en rättslig grund i GDPR. Bedömningen måste göras innan kamerabevakningen inleds. Om inte GDPR uppfylls finns risk för sanktionsavgifter.

Svenskt Näringsliv har nyligen publicerats en rapport som analyserar näringslivets utmaningar på dataskyddsområdet (*Vad är fel med GDPR*). Författarna av rapporten är Marin Brinnen, dataskyddsspecialist på Kahn Pedersen och Daniel Westman, oberoende rådgivare och forskare inom it- och medierätt. Författarna sammanfattar sina slutsatser bland annat genom att konstatera att GDPR har höjt medvetenheten om dataskydd men att arbetet inneburit ett omfattande administrativt arbete särskilt för företagen. De lyfter också fram bland annat att GDPR duger, att den svenska dataskyddslagen bör ses över och att Datainspektionens förebyggande verksamhet bör förstärkas. Det senare på grund av de stora kostnader som kan drabba företagen på grund av brister i regelverket och avsaknaden av vägledningar från Datainspektionen.

7.2.1 Lagar om samhällsviktiga tjänster

Det finns två lagar som ställer krav på leverantörer och verksamheter som behandlar samhällsviktiga tjänster. Små tillväxtföretag finns ofta inte i dessa sektorer, men om så är fallet måste dessa lagar beaktas:

- lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-lagen)
- säkerhetsskyddslagen

NIS-lagen gäller inte för verksamhet som omfattas av krav på säkerhetsskydd enligt säkerhetsskyddslagen. Dock om en verksamhet hos aktören faller under

säkerhetsskyddslagen kan andra delar av verksamheten fortfarande falla under NIS-lagen. Skillnaden mellan lagarna kan förenklat förklaras som att NIS-lagen omfattar samhällskritisk verksamhet på lokal nivå medan säkerhetsskyddslagen gäller på nationell nivå. Säkerhetsskyddslagen påverkar vanligtvis inte små tillväxtföretag men däremot kan NIS-lagen beröra privata och offentliga leverantörer som behandlar information inom energi, transporter, bankverksamhet, finansmarknadsinfrastruktur, hälso-och sjukvårdssektorn, leverans och distribution av dricksvatten och digital infrastruktur. Exempelvis har en av de intervjuade småföretagarna en affärsmodell som faller inom energisektorn och flera småföretagare i Sverige hanterar hälsovårdssystem med patientdata som faller under sjukvårdssektorn.

NIS-lagen innebär skyldigheter att ha ett ledningssystem för informationssäkerhet, inklusive ett kontinuitetshanteringssystem och en dokumenterad incidentrapportering.

7.3 Internationella lagar

I EU:s cybersäkerhetsstrategi där GDPR och NIS-direktivet ingår som en del har även i juni 2019 Cybersecurity Act trätt i kraft (Cybersecurity Act). Cybersäkerhetsakten är en förordning som dels fastställer mål, uppgifter och organisatoriska frågor som rör den Europeiska unionens cybersäkerhetsbyrå ENISA och dels innehåller bestämmelser om cybersäkerhetscertifiering. Genom förordningen inrättas det första EU-omfattande certifieringssystemet för att säkerställa att certifierade produkter, processer och tjänster som säljs i EU-länderna uppfyller relevanta krav inom cybersäkerhet. Företag kan använda den nya mekanismen för att certifiera produkter som till exempel uppkopplade bilar och smarta medicintekniska produkter. För små och medelstora företag och startups innebär certifieringen; minskat hinder för marknadsinträden, ett certifikat som "passar alla" - i hela EU, giltigt i såväl privat som offentlig sektor och certifierade lösningar kommer att ha en konkurrensfördel världen över. Det vill säga på sikt kan även mindre tillväxtföretag konkurrera med de större. Sverige har tillsatt en utredning som ska föreslå anpassningar i nationella bestämmelser (Regeringen, 2019d).

7.3.1 GDPR och CLOUD Act

En annan internationell lag som innefattar tillväxtföretag är den amerikanska CLOUD Act. Lagen innebär att amerikanska myndigheter kan begära ut data från amerikanska molnleverantörer och amerikanska leverantörer av olika slags elektronisk kommunikation, oavsett var i världen informationen och servrarna finns. Amerikanska myndigheter har med andra ord rätt att få tillgång till uppgifter om europeiska medborgare. Det står i strid med grundprinciperna för GDPR och innebär att säkerheten och integriteten för europeiska medborgares personuppgifter inte kan garanteras. Dock krävs att det föreligger stark misstanke om ett konkret brott för att myndigheten ska kunna begära ut uppgifterna.

Små tillväxtföretag som ofta använder amerikanska molntjänster för kostnadseffektiva lösningar, omfattas av lagen, men företagets informationsklassificering och riskanalys måste avgöra om amerikanska molntjänster ska användas eller inte.

7.4 Reflektioner

Bara under det senaste året har det kommit många nya regelverk – GDPR, NIS-lagen, säkerhetsskyddslagen och nu senast EU:s cybersäkerhetsakt. För ett litet tillväxtföretag kan det vara svårt att veta vilka lagar och regler som gäller den verksamhet som företaget bedriver. Osäkerheten kan leda till att man inte agerar på rätt saker, eller lägger ned för mycket resurser på sådant som inte är relevant för tillväxtföretaget.

Det upplevs som svårt att veta vilka lagar som det finns ett krav att anpassa sin verksamhet mot. Exempelvis finns en stor osäkerhet och debatt kring USA:s CLOUD Act, vilket egentligen inte påverkar många små tillväxtföretag emedan GDPR däremot har fått en stor påverkan på även mycket små tillväxtföretag beroende på deras verksamhet. Datainspektionens tillsynsverksamhet och beslut om böter kan också komma att få stor inverkan på tillväxtföretagen. Det talas idag om ”Andra vågen – GDPR” (ComputerSweden)

Ett litet tillväxtföretag har stora utmaningar när det gäller se till att det finns regler för vem som har tillgång till vad, hur det lagras och att lagar och regler efterlevs. Dessa frågor är inte prioriterade i någon större utsträckning om företagets primära produkt eller tjänst mer handlar om att driva den tekniska innovationen och digitaliseringen av verksamheten för att möta kundens behov och vara konkurrenskraftiga.

Ytterligare en effekt av GDPR är att de registrerade har rätt att begära skadestånd om de drabbats av skada till följd av en incident. Ännu har inte något skadeståndsfall enligt GDPR uppstått i Sverige. I Europa förbereds dock ett antal fall där skadeståndena förväntas bli långt större än de administrativa sanktionsavgifterna som påförts.

8 Tema 4. Ledarskap och digital spetskompetens

I Sverige har vi en brist på digital spetskompetens. En kartläggning som genomfördes av IT & Telekomföretagen, 2019 under 2017 visade på ett befarat underskott på 70 000 digitala experter år 2022.

Samtidigt visar undersökningar från Harvey Nash, 2019 att frågorna kring cybersäkerhet och digital innovation är de frågor som ökat allra mest de senaste åren när det gäller frågor som finns med på styrelsens agendor i större bolag. Det är en tidsfråga innan detta även avspeglas i små tillväxtföretags styrelser. Styrelsens sammansättning är viktig för att frågor kring digitalisering ska få fäste och genomslag i organisationen. Om fler än 3 personer i styrelsen innehar digital kompetens visar undersökningar på markant högre vinst och omsättningsökning än om två eller färre personer i styrelsen har digital kompetens (Sloan Management, 2019).

8.1 Strategisk spetskompetens ingen viktig fråga?

Av djupintervjuerna i detta projekt framgår att behoven av digital spetskompetens inte är en av de viktigare frågorna. De flesta har inte planer på att rekrytera spetskompetens inom området och om de behöver kompetens tar de in konsulter. De flesta vänder sig antingen till sitt branschförbund, till någon de tidigare har haft kontakt med eller till bekanta som kan lotsa dem vidare för att hitta kompetens. Även myndigheter och företagsfrämjare finns som kontaktytor för att hitta kompetens. De som inte vet var de ska vända sig anser att de vet för lite för att vara en bra beställare.

Ungefär hälften av de tillfrågade företagen anger att kompetensnivån i ledningen beträffande informationssäkerhet är låg eller obefintlig. De litar antingen på en särskilt utsedd funktion i företaget, oftast IT, eller på hostingföretag och systemleverantörer. Några av de intervjuade företagen har god eller mycket god kompetens för att det kravställs eller är intresserade av informationssäkerhet.

Idag är det samtidigt lätt att beställa IT-system. Det behövs inte en IT-chef för att genomföra en beställning, vilket medför att frågor om exempelvis genomförda riskanalyser, informationssäkerhetsklassningar och dokumenterade kontinuitetsplaner innan system köps in, installeras och kopplas upp mot internet inte kravställs. GDPR har väckt frågan om cybersäkerhet och digitala risker i många styrelser och ledningsgrupper, men styrelsen har inte haft förmågan att omvandla medvetenheten om risker till praktiska åtgärder. Rädslor har i många fall varit kopplade till sanktionsavgifter och skadestånd till drabbade individer och inte till risker med ett bristande informationssäkerhetsarbete.

8.2 Reflektioner

Den bild som Regeringen beskriver avseende behov av digital spetskompetens (Regeringen, 2019c) är inte samma bild som de intervjuade tillväxtföretagen uppger. Urvalet bland företag för studien var begränsat, men det ger en indikation på att den brist på spetskompetens som regeringen ser, inte riktigt märks hos tillväxtföretagen.

I de intervjuer som genomförts belyser man inte risken att med att få tillgång till digital spetskompetens som en av de större riskerna. Orsaken till detta kan bero på antingen att företagen:

- har tillgång till de kompetenser som de behöver
- har ett behov av en större förståelse för digitala affärsrisker och cybersäkerhet

Kartläggningen visar att kompetensnivån i ledning och styrelse beträffande informationssäkerhet är låg eller obefintlig. Det finns dock en ökad förståelse för att dessa frågor är viktiga. GDPR har väckt frågan i många styrelser och ledningsgrupper, men man förstår inte kopplingen till informationssäkerhet. Det går inte att följa GDPR:s krav fullt ut om man inte arbetar systematiskt med informationssäkerhet eftersom personuppgifterna som företagen hanterar inte får ett reellt skydd.

8.2.1 Liten yrkesgrupp

Traditionellt har antalet personer i Sverige som varit fullt sysselsatta med informationssäkerhet och liknande roller varit en relativt liten yrkesgrupp där det inte finns någon officiell siffra. Enligt LinkedIn finns i november 2019 drygt 2 900 personer som inkluderar ordet *informationssäkerhet* i sin titel. Motsvarande siffra för *IT-säkerhet* är 8 100 personer.

Det finns en ökande efterfrågan av digital expertkompetens som även gäller för roller som arbetar med informations- och cybersäkerhet och utbudet av personer som påbörjat en karriär inom området har också ökat.

Tillväxtföretag som har mognat i sin digitala resa och har behov av att stärka sin organisation med kompetens inom informations- och cybersäkerhet och digitala affärsrisker kan ha svårt att hitta den kompetens de söker om de avser att anställa. Det finns konsultbolag som erbjuder kompetens, i intervjuerna belyses det inte som ett problem att kompetens saknas när de behöver denna.

8.2.2 Informationssäkerhet bör vara en ledningsfråga

På många sätt är också systematiskt informationssäkerhetsarbete en del av organisationens kvalitetsarbete då man på så sätt får kontroll på risker, arbetar strukturerat med incidenter och utbildar personalen, vilket minskar risken för incidenter.

Om inte informationssäkerhet är en lednings- och styrningsfråga så prioriteras det inte heller i verksamheten. Styrsignaler som kommer uppifrån påverkar förutsättningarna för ett säkerhetsmedvetande på ett positivt sätt och kan till och med vara ett krav för ett lyckat införande.

Erfarenhetsmässigt är det mycket svårt att införa ett systematiskt arbete med informations- och cybersäkerhet i en organisation om ledningens stöd saknas eftersom införandet tar lång tid, kostar pengar och kräver oftast nya system/tjänster samt utbildning av personalen.

När en allvarlig incident har inträffat är det också av yttersta vikt att ha en bra krishantering för att skydda företagets varumärke och ekonomi, oavsett orsak till och konsekvens av incidenten.

Informationssäkerhetsfrågorna nämns som en prioriterad fråga för ca hälften av de intervjuade tillväxtföretagen. Ett fåtal av företagen har en beslutad informationssäkerhetspolicy. De som inte har prioriterat det förklarar det med att kunderna inte har de kraven och att man inte har varit utsatt för något dataintrång. Dock beskriver de att kundernas förtroende för dem är jätteviktigt.

Åsa Schwarz, författare och cybersäkerhetsexpert, om ledningens roll

Åsa arbetar som konsult på KnowIT Secure i Stockholm och är en populär förläsare och uttalar sig ofta som expert inom cybersäkerhet i media. Åsa fick svara på följande frågor kopplat till informationssäkerhet och cybersäkerhet för små tillväxtföretag.

Hur ska ledningen/styrelsen i små tillväxtföretag arbeta med omvärldsbevakning inom informationssäkerhet och cybersäkerhet?
Gartner och konsultbolag som t ex McKinsey gör bra övergripande sammanfattningar på ledningsnivå medan om de är intresserade av vissa expertområden och kontinuerligt vill följa utvecklingen, bör de skaffa ett eget flöde på Linkedin och Twitter som passar verksamheten. Det allra bästa är ofta att fråga någon i verksamheten som kan området eller för styrelsen att fråga VD hur bolaget arbetar.

Hur ökar man ledningens engagemang för frågor inom informations- och cybersäkerhet och vilken fördel ger det för små tillväxtföretag?
Först och främst är det en lönsamhetsfråga och det är det som skapar engagemang. Bolag med digital kompetens i styrelse och ledning är mer lönsamma (+ 17% källa: (MITSloan, 2019) och växer snabbare (+38%). En viktig del i digitaliseringen är cybersäkerhet vilket också ger bolag stora konkurrensfördelar om de redan tidigt i utvecklingsprocessen fattar strategiska beslut som är underbyggda med korrekt underlag inom juridik och cybersäkerhet. Sedan är det numera ofta ett kundkrav om de ska arbeta med stora organisationer där detta numera är en hygienfaktor vid upphandlingen. Slutligen skapar en fungerande riskprocess trygghet och bra beslut som långsiktigt bidrar till ett sunt och välmående företag.

Ser du kopplingar mellan små tillväxtföretags riskaptit och hantering av informations- och cybersäkerhetsfrågor, om så hur påverkar det styrelsen/ledningens sätt att fatta beslut?
Ja, jag tror det är en bidragande fråga men som snarare handlar om kompetens. Små bolag har ofta inte kompetens i cybersäkerhetsfrågor och väljer bort att skaffa sig den eftersom de lägger alla resurser på att få ut en ny tjänst eller produkt på marknaden. Det behöver inte vara fel beslut men det vet dessvärre inte om deras verksamhet är i linje med deras riskaptit eller inte.

Vilken är den största risken som små tillväxtföretag utsätter sig för idag inom informations- och cybersäkerhet?
Den största risken är bristen på medvetenhet. Övriga risker och typer av attacker är relativt lika med större bolag även om det är verksamhetsberoende och även handlar om hur mycket bolaget exponerats. Några vanliga risker är dåliga lösenord, osäker kod och medarbetare som kan råka ut för phishingattacker. Vi har vid flera tillfällen samarbetat med branschorganisationer som vill stötta sina medlemmar i cybersäkerhetsfrågor. När vi kommer till de som har lägst säkerhet är det en helt annan process än för övriga – vi först måste uppmärksamma ledningen på frågorna. Annars är alla andra insatser döfödda.

9 Tema 5. Internationell utblick

9.1 Europa EU

The EU Cybersecurity Act

Tanken är att öka EU-ländernas förmåga att svara upp mot de allt fler och mer avancerade cyberhoten genom att etablera ett ramverk för certifieringar av tjänster, system och utrustning inom IT-området. Detta kan bli lag i framtiden.

Möjligheter med Cybersecurity Act;

- Skapar lika villkor för företag, medborgare och samhälle
- Europa kan bli marknadsledande inom området, vilket ger en konkurrenskraftig fördel
- Det kan stödja den digitala inre marknaden om certifiering harmoniseras inom EU
- Det ger mer förtroende för konsumenterna och affärsmöjligheter

Cyber Security Act innehåller nya initiativ som bland annat syftar till att:

- Införa ett gemensamt EU-certifieringssystem för cybersäkerhet
- Skapa en effektiv EU-byrå för cybersäkerhet – ENISA
- Öka genomförandekraften i förhållande till NIS-direktivet och GDPR
- Utreda hur Cyber Security Act förhåller sig till CLOUD Act

Cybersäkerhetsreformen betraktas som en av de viktigaste delarna på vägen mot en gemensam digital inre marknad som omfattar hela EU.

ENISA
ENISA är EU:s nätverks- och informationssäkerhetsbyrå. ENISA står för European Union Agency for Network and Information Security men de betecknar sig numera som European Union Agency for Cybersecurity. ENISA publicerar en mängd olika rapporter om informationssäkerhetshot bland annat en årlig hotrapport (ENISA, 2019b) där de största cyberhoten och trenderna listas, se figur 6. I den senaste rapporten från 2018 ligger skadlig kod, web-baserade attacker, web-apps attacker, nätfiske, överbelastningsattacker och spam i topp av listan på de 15 vanligaste hoten.
Majoriteten av sådana hot är stigande och det visas stora förändringar.

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	→	1. Malware	→	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application	↑	3. Web Application	→	→
4. Phising	↑	4. Phising	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	→	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threats	→	9. Insider Threat	↓	→
10. Physical manipulation/ damage/theft/loss	→	10. Physical manipulation/ damage/theft/loss	→	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Trends: ↓ Declining → Stable ↑ Increasing

Ranking: ↑ Going up → Same ↓ Going down

Figur 6: Årlig rapport av ENISA om de vanligaste hoten och trenderna, där en jämförelse också görs med föregående år.

I en rapport från maj 2019 (ENISA, 2019c) har ENISA intervjuat startup-bolag inom NIS-sektorn (Network and Information Security), det vill säga leverantörer av samhällsviktiga och vissa digitala tjänster. Målgruppen för rapporten är nystartade NIS-företag och små och medelstora företag samt företagare intresserad av att etablera sig i NIS-sektorn. Rapportens avsikt är bland annat att hjälpa sådana företag att identifiera de viktigaste utmaningarna de kan möta i sin utveckling och på vilka sätt de kan adressera dem. Rapporten tar upp kompetensbristen, att många teknikföretagare saknar utbildning inom cybersäkerhet samt att det är svårt att hitta rätt cybersäkerhetskompetens på grund av bristen på lämpliga profiler (som utvecklare eller etiska hackare), kostnaden för dem på grund av konkurrensen samt att skickliga cybersäkerhetsexperter ofta lockas av avancerad innovation utanför EU.

9.2 Finland

Finland har i den publika sektorn Finish Transport and Communications Agency, National Cyber Security Center som är en statlig organisation för att stötta företag i sitt informationssäkerhetsarbete (NCSC-FI, 2019)

Flera företag i Finland erbjuder informationssäkerhet och konsulterande. Finnish Information Security Cluster (FISC) är en organisation som startats av flera informationssäkerhetsfirmor för att främja nationellt och internationellt samarbete inom informationssäkerhet (FISC, 2019). FISC har 70 medlemsorganisationer och merparten är små till medelstora företag som koncentrerar sig på information- och cybersäkerhetsteknologier.

I Finland används även information från European Union Agency For Cybersecurity, ENISA (ENISA, 2019a) och SANS som är en plattform för certifiering, säkerhetsutbildning och forskning (SANS, 2019).

9.3 Tyskland

Den 27 mars 2019 föreslog det tyska federala inrikesministeriet (GMI) ett nytt lagförslag (”utkast till proposition”) för en så kallad IT Security Act 2.0 (IT-SiG 2.0). Förslaget är avsett att försvara Tysklands roll som ledande nation inom IT-säkerhet. För att göra detta syftar IT-SiG 2.0 till att anpassa sig till den tekniska utvecklingen genom att stänga juridiska kryphål och utöka det befintliga regelverket.

9.4 Estland

Estland ligger först i National Cyber Security Index (NCSI) av 107 länder (e-estonia, 2019a). Estland är det mest avancerade cybersäkerhetslandet i Europa och erbjuder unik expertis inom forskning, ledning och utveckling av cybersäkerhetslösningar (Estonia, 2019a) och (Estonia, 2019b)

Estland jobbar mycket med digitalisering och har kommit långt med digitala lösningar och säkerhetslösningar inom myndighetstjänster (e-estonia, 2019b). Estland tillhör det land som är mest digitaliserade och ökar samtidigt snabbast.

Estland har även ett flertal cybersäkerhetsföretag som erbjuder informationssäkerhet på olika nivåer. Estland erbjuder även Cyber North som är ett accelerationsprogram tillsammans med tillväxtföretag fokuserad på cybersäkerhet (CyberNorth, 2019)

9.5 Storbritannien

Cyber Essentials stödjer organisationer, oavsett storlek mot cyberhot (Cyber Essentials, 2019). Cyber Essentials stöds av Storbritanniens regering. Certifiering i cybersäkerhet på olika nivåer erbjuds genom Cyber Essentials.

9.6 Reflektioner

Det finns nationella skillnader mellan länder vilken syn man har på informations- och cybersäkerhet. I Sverige har vi traditionellt en hög tilltro på myndigheter och samhällets organ. Ett exempel på detta är att ingen av de intervjuade objekten i undersökningen efterfrågade ytterligare information kring identitet eller syfte när vid djupintervjuerna.

Många företag i Sverige har generellt en högre digitaliseringsmognad och har således ett större behov av att skydda sina informationstillgångar.

Estland är ett land som utmärker sig när det kommer till digitalisering. Ett exempel där de kommit längre i sin digitalisering är att man genomfört digitala riksdagsval och att hela myndighetssfären är digitaliserad. I Estland finns ett antal initiativ identifierade som skulle vara av intresse att inspireras av när det gäller att hjälpa företag att digitalisera dig på ett säkert sätt, bland annat CyberNorth.

Åsa Schwarz om internationell utblick

Vilket land anser du är en föregångare för informationssäkerhet och cybersäkerhet och vad ska Sverige ta efter?
UK, Nederländerna och USA. Vad vi ska ta efter är tydligare krav på verksamheter om vad som är en basnivå för informationssäkerhet som man helt enkelt måste ha infört. Den ska specificeras på nationell nivå för alla samhällsviktiga funktioner, och den ska vara tillgänglig för alla andra att tillämpa om man vill.

10 Slutsatser & rekommendationer

Kartläggningen och intervjuerna med experter och företagsfrämjare bekräftar vår samlade erfarenhet att förståelsen för och kunskapen om informationssäkerhet är låg hos majoriteten av små tillväxtföretag. I dag ställs det inte några generella lagkrav eller krav från kunder, myndigheter och företagsfrämjare att informations- och cybersäkerhetfrågor ska vara en naturlig del i företagens kvalitetsarbete. Svenska företag har ett stort fokus på miljöfrågorna men det låg inte på agendan för bara ett par år sedan. En försiktig gissning är att det på samma sätt som med miljöfrågorna, kan krävas ett långsiktigt arbete att ingjuta informationssäkerhetsmedvetande hos företagen, där samhället i kombination med media kan bidra med regelverk, tillägg i läroplanen, information och riktade insatser. Utbudet av information och kompetens på området är stort men den stora utmaningen är att få företagen att inse ”What´s in it for me?”.

Okunskapen kring informations- och cybersäkerhetsrisker skapar omedvetna digitala affärsrisker som behöver lyftas fram och belysas. För att öka små tillväxtföretags beredskap kring digitala risker vill vi särskilt lyfta fram följande tre förbättringsområden;

- Ökad kunskap om informationssäkerhet hos företagsfrämjare så att de kan vara ett stöd till men också en kravställare på tillväxtföretagen. ”Lär lärarna”.
- Öka förståelsen i ledning och styrelse för hur informations- och cybersäkerhet är kopplat till företagets affärsrisker
- Verka för bättre beställarkunskap kring säkra IT-tjänster

10.1 Förslag på kunskapshöjande insatser

Rikta insatser mot företagsfrämjare för att prioritera och integrera digitala risker i sina erbjudanden

En viktig insats att öka kunskap om informations- och cybersäkerhet hos företagen är att ”lära lärarna”, det vill säga företagsfrämjarna, så att de senare kan vara ett stöd till men också en tydlig kravställare på företagen. Om företagsfrämjare och andra aktörer ställer krav på att frågor kring informations- och cybersäkerhet måste hanteras blir dessa frågor en naturlig del i kravställningen såsom ekonomi, kvalitet och miljö är.

Utveckla förutsättningar för att informations- och cybersäkerhet tydligt finns med i företagsfrämjarnas ordinarie verksamhetsprocesser, frågebatterier, checklistor och urvalskriterier när de vägleder och utvärderar företagen.

- Öka kunskapen bland företagsfrämjare
- Ta fram utvärderingsverktyg, checklistor och information om det utbud som finns
- Inspirera med certifieringar eller diplom för extra guldkant när företag tar sin an frågorna
- Arbeta utåtriktat med att identifiera företag som har stora behov och nytta av att arbeta med säkerhetsrelaterade frågor.

Engagera ledning och styrelse i små tillväxtföretag

Att engagera ledning och styrelse i dessa frågor kan vara nyckeln för små tillväxtföretag att börja jobba med informationssäkerhet.

- Verka för att marknadsföra certifiering eller diplomering av företagsfrämjare, branschorganisationer eller andra organisationer.
- Verka för riktade insatser mot ledning och styrelse genom seminarier, frukostmöten, företagsevent och dylikt. Visa på;
  - Goda exempel
  - Högre lönsamhet genom att undvika risker och böter.

Cybersäkerhetsprogram i samråd med tillsynsmyndigheter och specialister

Skapa acceleratorprogram för innovation och informationssäkerhet, utformat för att stötta små företag eller tillväxtföretag när de utvecklar innovativa produkter och tjänster. Programmen skulle bestå av team av kompetenser inom tillsynsmyndigheter, informationssäkerhet, dataskydd, juridik och verksamhet som ser till att risker förknippade med projektens användning av känslig information och personuppgifter minimeras. Programmen som bygger på att skapa en miljö kring samarbete skulle erbjudas på flera olika ställen i Sverige och syfta till att dels skapa rättssäkerhet kring genomförandet av innovation dels utmynna i kompetensöverföring och nätverkande kring frågorna. Programmet kan med fördel startas i pilotverksamhet för att utvärdera nyttan. Goda exempel på internationella förlagor är Estniska CyberNorth och engelska ICO:s Sandlåda.

Öka tillväxtföretagens kompetens och tillgång till cyberförsäkringar

En reaktiv men viktig åtgärd för små tillväxtföretag kan vara att teckna cyberförsäkringar. Behovet finns särskilt hos de företagen med låg informations- och cybersäkerhetsmognad. Särskilt viktigt är detta för företag med ett stort antal kunder eller tjänster som är känsliga för bristande tillgänglighet. En cyberförsäkring hjälper företaget att snabbare hantera konsekvensen av en incident som annars kan driva företaget i konkurs.

Konkreta åtgärder är att underlätta för tillväxtföretagen genom att:

- Subventionera cyberförsäkringar
- Ta fram informationsmaterial för cyberförsäkringar och tillväxtföretag.

10.2 Vikten av ett långsiktigt hållbart digitalt företagande

Ett långsiktigt digitalt hållbart företagande innebär att ett företag har möjlighet att klara av att motstå flera av de risker som digitaliseringen innebär.

Digitaliseringens informationssäkerhetsrisker bör därför fortsätta att synliggöras och metoderna för att upptäcka och undvika dem lyftas fram. Visa på goda exempel på hur de som har lyckats har gjort. Det kan göras i olika informationsinsatser om var stöd, information och rådgivning finns, exempelvis Stöldskyddsföreningens självtest.

Verka för utlysningar och andra insatser som driver på säkerhetsmedvetenheten exempelvis genom verktyg som ”Informationssäkerhet for Dummies”, paket för prioriterade åtgärder (lägstanivå för informationssäkerhet), metoder för mognadsklassificering och liknande.

Avslutningsvis kan den privata marknaden av utbud ges incitament till att synliggöra och paketera prisvärda tjänster för nystartade och små tillväxtföretag.

11 Referenser

ACM Code of Ethics and Professional Conduct
https://www.acm.org/binaries/content/assets/about/acm-code-of-ethics-booklet.pdf

Aon, 2019. Hur utsatt är du och ditt företag för cyberrisker?
https://www.aon.com/sweden/produkter-tjanster/riskhantering/cyberforsakring.jsp

Allianz Risk Barometer, Top business risks for 2019
https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2019.pdf

ComputerSweden, Arg på digitaliseringshinder? Så kan lagen bli ett stöd i stället
https://computersweden.idg.se/2.2683/1.723300/digitaliseringshinder-lagen-stod?utm_source=dmdelivery&utm_medium=email&utm_campaign=IDG%20Senaste%20nytt%20Morgon%202017%202019-09-25%207%3A46%3A19

ComputerSweden, Andra vågen – GDPR åter högt på företagens agendor
https://computersweden.idg.se/2.2683/1.725679/gdpr-andra-vag

CIS, 2019. CIS Controls
https://cybernetsecurity.com/industry-papers/CIS-Controls%20Version-7-cc-FINAL.PDF

Cygate, 2019. Cybersäkerhet - en helhet av lösningar
https://www.cygate.se/vi-erbjuder/cybersakerhet/

Cyber Essentials, 2019. National Cyber Security Center
https://www.cyberessentials.ncsc.gov.uk

CyberNorth, 2019. Defense AI and cybersecurity focused accelerator by Startuo Wise Guys together with Estonian Defence Industry Association and Estonian Ministry of Defence
https://startupwiseguys.com/cybernorth/

Cybersecurity Act
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

Datainspektionen, 2019. Datainspektionen.
https://www.datainspektionen.se/

DinSäkerhet.se, 2019a. Tänk Säkert
https://www.dinsakerhet.se/

DinSäkerhet.se, 2019b. Spellista informationssäkerhet
https://www.youtube.com/playlist?list=PLC30065439492B727

e-estonia, 2019a. Estonia takes the top spot in the National Cyber Security Index.
https://e-estonia.com/estonia-takes-the-top-spot-in-the-national-cyber-security-index/

e-estonia, 2019b. We have built a digital society and so can you
https://e-estonia.com

EDPBs och EDPSs svar om Cloud Act
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_edps_joint_response_us_cloudact_coverletter.pdf

Enforcementtracker.com
https://enforcementtracker.com/

ENISA, 2019a. European Union Agency for cybersecurity
https://www.enisa.europa.eu

ENISA, 2019b. Threat Landscape Report
https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

ENISA, 2019c. From start-up to enterprise: ENISA's recommendations on building EU cyber-champions
https://www.enisa.europa.eu/news/enisa-news/from-start-up-to-enterprise-enisas-recommendations-on-building-eu-cyber-champions

Estonia, 2019a. How Estonia became a global heavyweight in cyber security
https://investinestonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/

Estonia, 2019b. Cyber Security
https://investinestonia.com/business-opportunities/cyber-security/

FINRA Cybersecurity checklist
https://www.finra.org/compliance-tools/cybersecurity-checklist

FISC, 2019. Finnish Cyber Security, no strings attached
https://www.fisc.fi/en

GDPR, EU:s dataskyddsförordning
https://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX:32016R0679&rid=1

Harvey Nash, 2019. The uncomfortable boardroom – the new normal
https://www.harveynash.com/boardresearch/

ICO, 2019. ICO opens Sandbox beta phase to enhance data protection and support innovation.
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/03/ico-opens-sandbox-beta-phase-to-enhance-data-protection-and-support-innovation/

Internetstiftelsen, 2019
https://internetkunskap.se

ICO, ICO selects first participants for data protection Sandbox
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-selects-first-participants-for-data-protection-sandbox/

MITSloan, 2019. It Pays to Have a Digitally Savvy Board
https://sloanreview.mit.edu/article/it-pays-to-have-a-digitally-savvy-board/

MSB med flera, 2019 Tänk säkert – skydda din viktigaste information! Att stärka allmänhetens samt små och medelstora företags motståndskraft mot IT-incidenter
https://www.msb.se/siteassets/dokument/om-msb/vart-uppdrag/regeringsuppdrag/2019/att-starka-allmanhetens-samt-sma-och-medelstora-foretags-motstandskraft-mot-it-incidenter-2019.pdf

MSB, 2019a. Informationssäkerhet för små företag – Rekommendationer för dig som driver eget företag med upp till 10 anställda
https://rib.msb.se/filer/pdf/28741.pdf

MSB, 2019b Grundläggande it-säkerhetsåtgärder
https://www.informationssakerhet.se/siteassets/nyheter/vagledning---grundlaggande-it-sakerhetsatgarder---forhandsutgava.pdf

MSB, 2019c. Datorstöd informationssäkerhetsutbildning för användare (DISA)
https://www.msb.se/sv/utbildning--ovning/alla-utbildningar/datorstodd-informationssakerhetsutbildning-for-anvandare-disa/

MSB, 2019d. Grundläggande säkerhetsskyddsutbildning via webben
https://www.msb.se/sv/utbildning--ovning/alla-utbildningar/ny-sidagrundlaggande-sakerhetsskyddsutbildning-via-webben/

MSB, 2019e. Metodstöd för informationssäkerhet
https://www.informationssakerhet.se/metodstodet/

MSB med flera 2019, Nationell handlingsplan för samhällets informations- och cybersäkerhet
https://rib.msb.se/filer/pdf/28804.pdf

NCSC-FI, 2019. Welcome to the NCSC-FI website!
https://www.kyberturvallisuuskeskus.fi/en

NIST, 2019. Cybersecurity Framework.
https://www.nist.gov/cyberframework

NIST DRAFT 2019, Privacy Framework
https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2019/09/nist_privacy_framework_preliminary_draft.pdf

Nixu, 2019. Informationssäkerhetstjänster från Nixu
https://www.nixu.com/sv/all-services

Regeringen, 2017 För ett hållbart digitaliserat Sverige - en digitaliseringsstrategi
https://www.regeringen.se/49adea/contentassets/5429e024be6847fc907b786ab954228f/digitaliseringsstrategin_slutlig_170518-2.pdf

Regeringen, 2018a Uppdrag till Tillväxtverket att utveckla och genomföra ett program för att höja kompetensen om digitalisering i små företags ledningar och styrelser
https://tillvaxtverket.se/download/18.2da96e791651617ef30a11c1/1534419924737/Uppdrag%20att%20utveckla%20kompetens%20om%20digitalisering%20i%20små%20företags%20ledningar%20och%20styrelser.PDF

Regeringen, 2018b Nationell strategi för samhällets informations- och cybersäkerhet
https://www.regeringen.se/regeringens-politik/krisberedskap/nationell-strategi-for-samhallets-informations--och-cybersakerhet/

Regeringen, 2018c Uppdrag till Myndigheten för samhällsskydd och beredskap att stärka allmänhetens samt små och medelstora företags motståndskraft mot IT-incidenter
https://www.regeringen.se/49571d/contentassets/da4b5250ae414d5e94cfe406f3ddfce0/uppdrag-till-myndigheten-for-samhallsskydd-och-beredskap-att-starka-allmanhetens-samt-sma-och-medelstora-foretags-motstandskraft-mot-it-incidenter

Regeringen 2018d Uppdrag om en samlad informations- och cybersäkerhetshandlingsplan för åren 2019–2022
https://www.regeringen.se/regeringsuppdrag/2018/07/uppdrag-om-en-samlad-informations--och-cybersakerhetshandlingsplan-for-aren-20192022/

Regeringen, 2019a Uppdrag till Tillväxtverket att främja små och medelstora företags förmåga att använda data som strategisk resurs
https://www.regeringen.se/4a43e5/contentassets/fc317c477e0246c28e64c2da2862794f/uppdrag-att-framja-sma-och-medelstora-foretags-formaga-att-anvanda-data-som-strategisk-resurs.pdf

Regeringen, 2019b Uppdrag inför inrättandet av ett nationellt cybersäkerhetscenter
https://www.regeringen.se/4a7f68/globalassets/regeringen/dokument/forsvarsdepartementet/regeringsbeslut/uppdrag-infor-inrattandet-av-ett-nationellt-cybersakerhetscenter.pdf

Regeringen, 2019c. Uppdrag att samverka kring kompetensförsörjningen av digital spetskompetens
https://www.regeringen.se/regeringsuppdrag/2019/08/uppdrag-att-samverka-kring-kompetensforsorjningen-av-digital-spetskompetens/

Regeringen, 2019d
https://www.regeringen.se/pressmeddelanden/2019/10/utredning-tillsatts-om-svensk-anpassning-till-eus-cybersakerhetsakt-och-om-vissa-atgarder-till-skydd-for-verksamheter-av-betydelse-for-sveriges-sakerhet/

RISE Stresstest
https://www.ri.se/sv/press/rise-oppnar-testbadd-cybersakerhet

SANS, 2019. The most trusted source for information security training, certification and research
https://www.sans.org

SIS-TR 50:2015
https://www.sis.se/api/document/preview/8014024/

Sloan Management, 2019. MITSLOAN Management Review
https://sloanreview.mit.edu

Stöldskyddsföreningen, 2019a. Certifiera ditt företag
https://www.ssfcybersäkerhet.se/om-certifiering/

Stöldskyddsföreningen, 2019b. Guide till grundläggande cybersäkerhet
https://www.ssfcybersäkerhet.se/sakerhetsguide-for-it-sakerhet/

Stöldskyddsföreningen, 2019c. SSF Cybersäkerhet Bas- lär dig grundläggande IT-säkerhet.
https://www.stoldskyddsforeningen.se/foretag/utbildningar/ssf-cybersakerhet-bas---grundlaggande-it-sakerhet/

Svenskt Näringsliv, Vad är fel med GDPR
https://www.svensktnaringsliv.se/migration_catalog/Rapporter_och_opinionsmaterial/Rapporter/vad-ar-fel-med-gdpr_747901.html/BINARY/Vad%20%C3%A4r%20fel%20med%20GDPR-.pdf

Swedac, sök ackrediterade organ
https://www.swedac.se/tjanster/ackreditering/sok-ackrediterade-organ/

Tillväxtverket, 2019. Digital kompetens för affärsutveckling. Senast uppdaterad: 2019-08-20
https://tillvaxtverket.se/amnesomraden/digitalisering/digital-kompetens-for-affarsutveckling.html

Verksamt.se, 2019. Informationssäkerhet
https://www.verksamt.se/starta/skydda-ditt-foretag/informationssakerhet

Tillväxtverket
Swedish Agency for Economic
and Regional Growth
Tel 08-681 91 00
tillvaxtverket.se

Tillväxtverket arbetar för hållbar tillväxt och konkurrenskraftiga företag i alla delar av Sverige. Det gör vi genom att stärka företag och regioner. Vi erbjuder kunskap, nätverk och finansiering. Det ger direkt nytta till företag, och också förutsättningar för företag och regioner att möta framtidens utmaningar. Tillväxtverket är en nationell myndighet med regional närvaro på nio orter. Ett Sverige med fler företag som vill, kan och vågar är vår vision.

tillväxt
verket