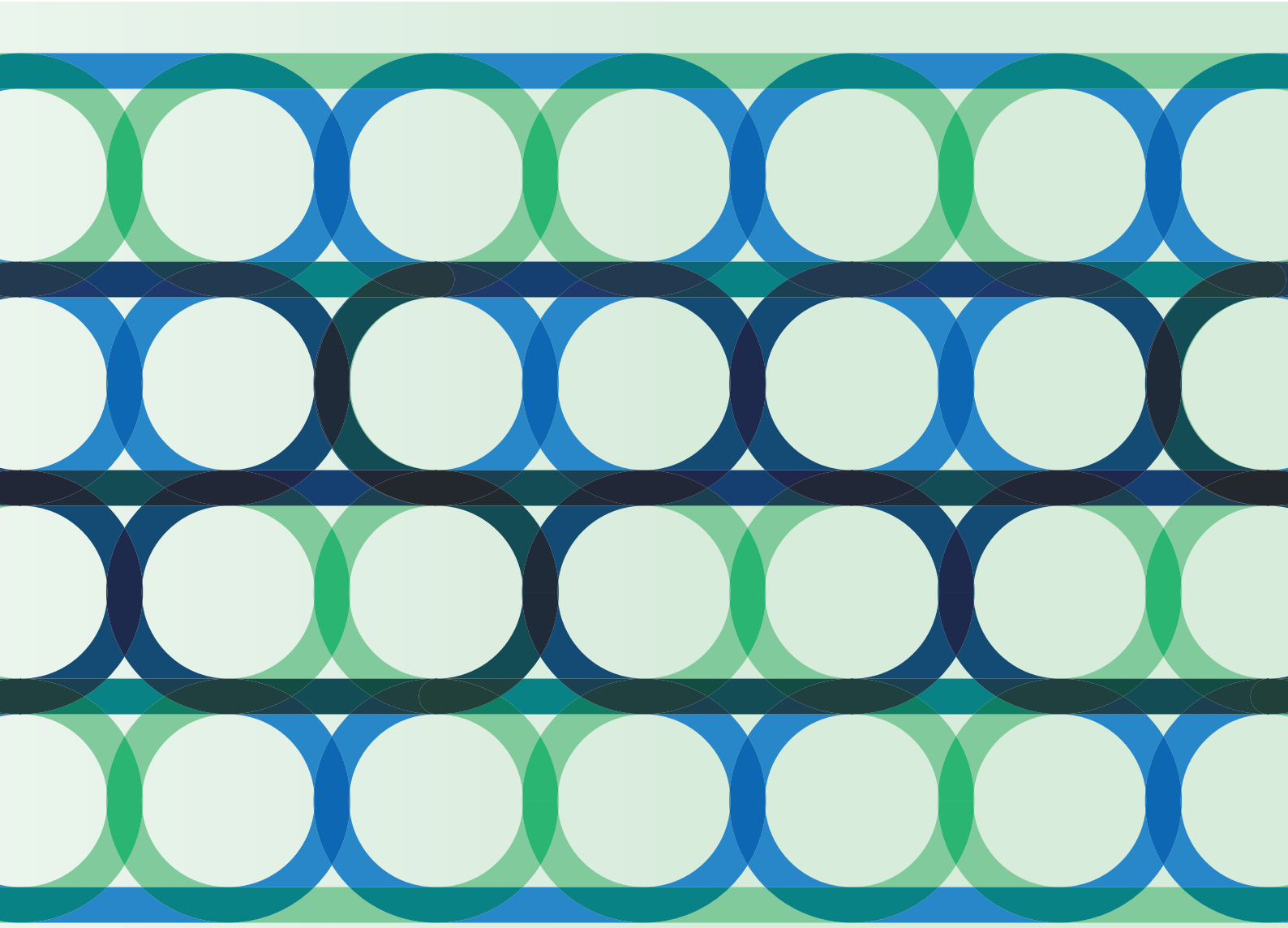
Branschrapport SFM 2023

Cyberrisker, försäkring och försäkringsförmedling

Hur bidrar branschen till ett samhällsviktigt område?



Svenska försäkringsförmedlares förening

SFM (Svenska försäkringsförmedlares förening) är branschorganisationen för försäkringsförmedlare (inom liv- och sakförsäkring) i Sverige med cirka 2000 individuella medlemmar fördelat på 110 förmedlarorganisationer. SFM verkar för en försäkringsförmedlarbransch med hög kvalitet och god konkurrens på försäkringsmarknaden och 2012 etablerades InsureSec som är ett branschregleringsorgan för en stark självreglering.

SFM arbetar proaktivt med kunskapsspridning till viktiga intressenter på både nationell och internationell nivå för att utveckla branschen. Att vara SFM-medlem ska innebära en kvalitetsstämpel för kunder och för de försäkringsbolag som samarbetar med förmedlarna. SFM är medlem i BIPAR, The European Federation of Insurance Intermediaries, som representerar 800 000 försäkringsförmedlare i Europa.

Innehåll

1 Inledning

1.1 Varför en branschrapport om cyberrisker, försäkring och försäkringsförmedling?

Cyberhotet, de risker det medför och de incidenter det orsakar, är idag en stor del av vår vardag och vårt samhälle. Cyberhotbilden och dess konsekvenser påverkar hela samhället, från den enskilda individen, till företag och samhällsviktiga aktörer såsom myndigheter, kommuner, regioner - och ytterst riksdag och regering. Trots den stora påverkan som cyberhotet har på samhället finns det fortfarande stora kunskapsluckor hos företag, myndigheter och andra samhällsaktörer kring proaktivt skyddsarbete och möjligheten till att försäkra sig mot riskerna.

Den här branschrapporten är framtagen av Svenska försäkringsförmedlares förening (SFM), branschorganisationen för försäkringsförmedlare i Sverige, tillsammans med det svenska cybersäkerhetsföretaget Truesec som är verksamma internationellt. Deltagande försäkringsbolag och förmedlarbolag inom SFM:s Forum för Sakförsäkring har även bidragit till rapporten genom en utsedd referensgrupp. Ett särskilt tack vill SFM rikta till Marsh McLennan, Söderberg & Partners, If, Dina Försäkringar, Trygg-Hansa och Säkra.

1.2 Vem riktar sig rapporten till?

Rapporten är framtagen för relevanta beslutsfattare i privat och offentlig sektor för att öka förståelsen för cyberhot, cyberrisker och incidenter. Rapporten ger även en bild av varför cyberförsäkring och försäkringsförmedling är en viktig del i det proaktiva arbetet för att möta dessa hot, hantera riskerna och minimera incidenterna för svenska företag och samhället som helhet. Rapporten är en första version och syftet är att framöver arbeta vidare med innehållet i takt med förändringar som sker för att kunna göra uppdaterade versioner.

1.3 Sammanfattning- Kunskap, samverkan och cyberförsäkring för ett mer motståndskraftigt samhälle och företagande i Sverige

Cyberrisker har sitt upphov i medvetet agerande av någon som har ont uppsåt. Att försäkra dessa risker är därför av sin natur utmanande eftersom försäkring avser risker som är förknippade med slumpartade händelser. Riskerna är emellertid inte oförsäkringsbara utan det finns en marknad för försäkring mot cyberrisker.

Intresset för cybersäkerhet har ökat kraftigt de senaste åren i takt med att antalet cyberattacker och brott ökat lavinartat. Cyberförsäkring, eller också kallat databrottsförsäkring, skyddar ett bolags ekonomi, ansvar, data och digitala tillgångar vid datasäkerhetsrelaterade incidenter.

Branschen (försäkringsförmedlarbolag och försäkringsbolag som arbetar med försäkringsförmedlare) har gemensam uppgift att hjälpa företag att försäkra sig mot risker de mötet i sin verksamhet.

Genom att hjälpa företag överföra vissa typer av risker till försäkringbolag, exempelvis cyberrisker, ser försäkringsförmedlare till att företag inte begränsas eller hindras till följd av dessa risker, utan företagen kan i stället fokusera på sin verksamhet.

Idag erbjuder tre av de fyra stora svenska försäkringsbolagen cyberförsäkring till företag. Försäkringsförmedlare kan bidra till försäkringsbolagens produktutveckling genom försäkringsförmedlarens insikt i aktuella marknadsförflyttningar och kundbehov. Försäkringsförmedlarna har även en viktig roll i att identifiera nya risker och hitta gap i utbudet på försäkringsmarknaden och arbeta för en sund utformning av produkter

för företagen. Cyberförsäkring är ett exempel på en sådan utveckling där förmedlarna aktivt driver behovet av att utveckla försäkringar kopplade till cybersäkerhet.

Den förmedlade sakförsäkringsmarknaden uppgick till cirka 27 miljarder SEK i inbetalda premier under 2021 och växte med 13 % mellan 2020 och 2021. Cirka 800 miljoner SEK av dessa premier är att hänföra till cyberförsäkring som förmedlas i Sverige.

Sverige är ett av världens mest digitaliserade länder samtidigt som vi släpar efter med den digitala säkerheten. Utifrån Truesecs erfarenhet är IT sällan identifierat som ett verksamhetskritiskt område utan är ofta nedprioriterat och betraktas allt som oftast som en kostnadspost snarare än en förmåga för att driva utveckling. Cyberrisker behöver betraktas som en affärsverksamhetsrisk och kan inte ses som en isolerad IT-säkerhetsfråga. Företagens förmåga att skapa samverkan mellan verksamhet och IT kommer att vara avgörande för företagets motståndskraft.

I och med digitaliseringen kan alla branscher drabbas. Det finns idag nästintill ingen verksamhet som kan vara verksam om IT-och systemlösningarna slås ut. Det spelar inte någon roll om verksamheten bedriver hemtjänst, energiproduktion, tillverkning, logistik eller butiksförsäljning.

Det finns flera viktiga frågor för beslutfattare att agera på i frågan om cyberhotet. Den första och största frågan är att skaffa insikt och kunskap i ämnet. Sverige är ett digitalt samhälle och utan tillräcklig IT-kunskap försvåras beslutsfattandet. Att även säkerställa att medborgarna får en utbildning inom IT från en tidig ålder skulle bidra till att Sverige även i framtiden kan vara en konkurrenskraftig IT-nation. Den privata sektorn har idag större kapacitet och förmåga att driva frågor inom IT än den offentliga sektorn. Ett samarbete mellan den privata och offentliga sektorn i syfte att kunna bidra till samhället, där den privata sektorn kan vara drivande, behöver utvecklas för att kunna möta samhällets behov i framtiden.

För att göra Sveriges samhälle mer motståndskraftigt behövs större satsningar på utbildning och kunskap inom cyberhot och cyberrisker.

2 Hotbilden kopplat till cyberrisker

SFM HAR SAMMANSTÄLLT offentlig tillgänglig information om hotbilden och, har med hjälp av Truesec, sammanställt de erfarenheter som byggts upp över tid vad gäller hotbilden.

2.1 Cyberhotet

Sverige är ett av världens mest digitaliserade länder samtidigt som vi släpar efter med den digitala säkerheten. Utifrån Truesecs erfarenhet är IT sällan identifierat som ett verksamhetskritiskt område utan är ofta nedprioriterat och betraktas allt som oftast som en kostnadspost snarare än en verksamhetsmöjliggörande förmåga. Detta har lett till att digitaliseringen oftast drivs av verksamheten snarare än av IT-avdelningen och ofta utan insyn från IT-säkerhetsspecialister. Det är även så att denna förflyttning lett till att budgeten kopplat till digitalisering allt som oftast endast innehåller poster för utveckling, medan fortlöpande underhåll och för den delen avveckling glöms bort eller inte adresseras. Detta i sig leder till en av de största sårbarheterna i IT-miljöer av idag, nämligen problematiken kring föråldrade eller dåligt underhållna IT-system. Föråldrade system utvecklades med sin tids hot i åtanke, inte dagens alltjämt mer avancerade angreppsmetoder. Dåligt underhållna system uppdateras inte med de senaste uppdateringar kring säkerhetsförmågor. Resultatet är att det blir förhållandevis enkelt för en hotaktör att ta sig in i systemet, och därigenom även erhålla åtkomst till den övriga IT-miljön. Under 2023 bedöms cyberrisker vara bland de 10 största riskerna i världen (plats 8), såväl på kort sikt (2 år) som på lång sikt (10 år).[1]

1 Global Risk Report 2023, Word Economic Forum

När pandemin inträffade 2020, och alla verksamheter tog ett stort kliv över en natt för att möjliggöra distansarbete för anställda, blomstrade affärerna för de bakomliggande hotaktörerna. Europa var under 2021 den näst största attackerade regionen i världen[2]. Den totala kostnaden för skador orsakade av cyberkriminalitet för 2021 var 7 biljoner USD[3]. Utpressning (inklusive ransomware) stod för 38 procent av skadorna från företag under 2021[4]. Vidare förväntas attackerna öka med femton procent per år och kommer uppskattningsvis uppgå till 10,5 biljoner USD 2025. Med en affärsmässig ansats började hotaktörerna skala upp och specialisera sin affär. Detta innebar bland annat att några aktörer specialiserade sig på att utveckla skadlig kod som kunde användas för digitala intrång eller utveckling av molntjänster för ransomware eller överbelastningsattacker. Andra specialiserade sig på att utföra själva instegen i verksamheters digitala miljöer för att sedan auktionera ut åtkomsten till högstbjudande på handelsplatser i det så kallade Darknet. Köpare av dessa olika tjänster och förmågor är sedan den utförande hotaktören av den slutgiltiga attacken mot vald verksamhet.

Allt detta resulterade i att en utförande hotaktör behöver nästan ingen kompetens alls inom IT för att göra det som tidigare ansågs vara avancerade digitala angrepp. Att köpa dessa tjänster eller förmågor är dessutom inte heller kostsamt och kan i vissa fall vara helt kostnadsfritt. Den bakomliggande hotaktören kan ta ut en procentsats av den utförande partens intjäning, vilken oftast utgörs av lösensummor eller försäljning av information som införskaffats vid angreppet.

Riskerna som är förknippade med digital brottslighet är i förhållande till belöningen relativt låga. Anledningen till detta är att vissa länder inte agerar mot digitala brott så länge det inte drabbar det egna landets intressen. Ryssland är där ett tydligt exempel. Andra länder, exempelvis Nordkorea, har digitala brott som en inkomstkälla till nationalekonomin. Så länge hotaktören befinner sig i något av dessa länder, och inte avser att lämna landet, är lagföring för digitala brott låg.

Frekvensen av cyberincidenter för företag med en omsättning större än 500 miljoner euro ökade i en lägre takt än för företag med en omsättning lägre än 500 miljoner euro. Det beror antagligen på att de större företagen har bättre möjligheter att investera mer i cybersäkerhet och motståndskraft. Mellan 2019- 2021 ökade krav på skadeersättningar med 90 procent för företag med en omsättning under 500 miljoner euro, medan det för företag med omsättning större än 500 miljoner euro ökade med 26 procent.[5]

2 Marsh: Source: ENISA Threat Landscape 2022, IBM Cost of Breach Report 2022, IBM Threat Intelligence 2022, Verizon DBIR 2022

3 Cyber Crime Magazine, augusti 2022, 'Boardroom cybersecurity 2022 report' Cybersecurity Ventures

4 The Changing face of cyber claiming 2022, Marsh October 2022

5 The Changing face of cyber claiming 2022, Marsh October 2022

Utöver hotet från digital brottslighet behöver svenska verksamheter även beakta hoten från:

- digitalt industrispionage
- digital aktivism/påverkan och
- digital krigföring.

Dessa hot använder i stort samma tekniker och metoder men med väldigt olika syften.

Industrispionage upptäcks sällan då det utförs av avancerade grupper, såsom vissa länders egna underrättelsetjänster. Deras mål är att inte upptäckas och angreppen utförs under en lång tidshorisont. Informationen de stjäl säljs sedan till högstbjudande (om det är en privat hotaktör) eller ges bort till den egna nationens företag eller organisationer (om det är en statlig hotaktör).

Digital aktivism, påverkansoperationer och digital krigföring har som syfte att skapa oro eller försvaga en nation, både till förmåga och motståndsvilja. Rysslands invasionskrig av Ukraina visade hur djupt samarbetet mellan digital och hybridkrigsföring är. Det är också det första kriget där den digitala striden möjliggör för sympatisörer globalt att bidra i angrepp och försvar. De digitala påverkansoperationerna har även visat sig i Sverige i samband med att ryska sympatisörer under falsk flagg (Anonymous Sudan) angripit svenska verksamheter med överbelastningsattacker.

2.2 Branscher föremål för cyberhotet

IT är idag grunden för i stort sett alla verksamheter och i dagens Sverige sitter även de allra flesta verksamheter ihop. Samhället är ett mycket komplext system där exempelvis en stor del av den utförande verksamheten inom offentlig verksamhet drivs av bolag i privat regi. Det medför att den digitala brottsligheten inte drabbar en specifik bransch utan snarare så är den gemensamma nämnaren att det bedrivs en digital verksamhet i någon form. Med dagens digitalisering innebär detta att alla branscher drabbas. Det spelar inte någon roll om verksamheten bedriver myndighetsutövning, hemtjänst, energiproduktion, tillverkning, logistik eller butiksförsäljning.

Kostnaden för en cyberincident uppgår ofta till värdet av stillestånd i flera veckor av verksamheten. Men frågan rörande cyberangreppskostnader är även större än det rent finansiella. Angrepp mot offentlig verksamhet kan allvarligt påverka myndighetsutövning men också påverka samhällsfunktionen i sig – i individperspektivet t.ex. möjligheten till stöd och vård, vattenförsörjning och värmeleveranser. Denna typ av extraordinära konsekvenser kan medföra allvarliga konsekvenser för allmänhetens förtroende för myndigheterna.

Det här gör det även utmanande i ett riskmitigerande försäkringsperspektiv – det är inte bara det drabbade företagets avbrotts- och hanteringskostnader som behöver vägas in utan även störningar i samhällssystemet. Ett exempel i närtid är den leverantörsstörning som allvarligt påverkade A-kassornas förmåga att leverera på sitt samhällsviktiga uppdrag. Frågan om hur cybersäkerheten ska planeras och koordineras är därmed en viktig samhällsfråga som behöver koordineras på nationell nivå.

För att visa på beredskapen av skydd mot och relevansen av cyberhot i offentlig verksamhet har SFM gjort en sammanställning av tillgänglig information i årsredovisningar från år 2021 för Sveriges samtliga regioner. Nyckelord som använts är Cyber, IT-säkerhet, Informationssäkerhet, Säkerhet, samt Dataskydd. Av 21 regioner tog endast sex regioner upp begreppen cyber- eller informationssäkerhet som refererade till specifika områden samt presenterade en konkret handlingsplan. 9 av 21 regioner tar överhuvudtaget inte upp säkerhet inom cyber, IT eller information i sin årsredovisning.

2.3 Möjliga åtgärder för att möta cyberhotet

Kunskapen om både hotbilden i sig liksom de sårbarheter och beroenden som finns både inom det egna företaget och samhället i stort behöver öka – hos beslutsfattare på alla nivåer liksom hos varje medarbetare och medborgare. Det behöver även finnas en tydlig strategi i det arbete som görs för att öka företags och samhällets förmåga att hantera ett verkställt angrepp. För att stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera cyberhot har Försvarets radioanstalt (FRA), Försvarsmakten, Myndigheten för samhällsskydd och beredskap (MSB) och Säkerhetspolisen inrättat ett Nationellt Cybersäkerhetscenter på uppdrag av regeringen.

För att kunna möta cyberhotet behövs det byggas en förmåga att kunna upptäcka ett angrepp, en förmåga att kunna hantera det och att kunna återställa IT-miljön för att kunna återfå systemfunktionen.

Enligt Truesecs erfarenhet är följande viktigt för att upptäcka angrepp:

- En aktiv säkerhetsmonitorering av IT-miljön, dygnet runt.
- Ha kontroll över vilka som faktiskt har tillgång till IT- miljön. Aktiv och ständig användarhantering, som ger rätt behörigheter till rätt person i rätt situation, är viktig.

Vidare menar Truesec att för att kunna hantera ett angrepp och återställa miljön så effektivt som möjligt behövs:

- En tydlig specialistkompetens inom cyberkrishantering samt fungerande säkerhetskopior som går att återläsa.
- Väl utarbetade och testade kontinuitetsplaner hos verksamheterna för att kunna verka under den tid som IT-miljön och systemfunktionen är påverkad.

För att möta cyberhoten behöver det även enligt Truesec finnas:

- Ett aktivt IT-säkerhetsarbete som är väl avvägt mot hotbilden.
- Kunskap och riskmedvetenhet. Alla verksamheter, oavsett sektor och storlek, behöver säkerställa att kompetensen finns, inom egen organisation eller hos leverantör, för att faktisk upptäcka, hantera och återställa funktion, och verksamhetskonsekvenserna behöver mitigeras genom kontinuitetsplanering i kombination med lämpligt försäkringsskydd.

Utifrån ett försäkringsperspektiv är det bara en tidsfråga innan cyberförsäkring ingår som en naturlig del av ett försäkringserbjudande, både för privatpersoner och för företag. Detta utöver samarbeten och att arbeta proaktivt för att säkerställa att företagen har så bra skydd de kan ha innan en eventuell cyberattack sker. Många försäkringsbolag tar till exempel fram utbildningar inom riskhantering och kan också bistå med t.ex. Password Manager eller andra riskförbättrande åtgärder. Vissa försäkringsbolag gör scanning av kundmiljö som också delas eller erbjuder skadeförebyggande åtgärder som antivirus/brandvägg/back-up-abonnemang som del av försäkringen då dessa åtgärder krävs som minikrav även hos de minsta företagen.

3 Cyberförsäkring och försäkrings-förmedling

FÖRSÄKRINGSPRODUKTER för cyberrisker är relativt nytt på försäkringsmarknaden jämfört med de flesta andra försäkringstyperna.

Cyberförsäkring, eller också kallat databrottsförsäkring, ska likt andra försäkringar skydda ett bolags ekonomi, data och digitala tillgångar vid en cyberincident. En del som dock skiljer sig från många andra försäkringstyper är att cyberförsäkringen normalt även innefattar en aktiv del i form av tillgång till en dygnet-runt koordinator som i sin tur har tillgång till en grupp av sakkunniga leverantörer inom ex. IT, juridik eller PR, redo att rycka ut beroende på vilken typ av incident om inträffat.

3.1 Cyberförsäkring i Sverige

Tre av de fyra stora svenska försäkringsbolagen på försäkringsmarknaden erbjuder i dagsläget cyberförsäkring till sina kunder och den fjärde håller på att utveckla ett sådant försäkringserbjudande. Cyberförsäkring erbjuds ofta av försäkringsbolagen som ett komplement till en företagsförsäkring. Stora eller mer tekniskt komplexa företag har möjlighet att teckna cyberförsäkring stand-alone hos vissa försäkringsbolag. För stora företag skräddarsys eller begränsas dessutom försäkringsskydd i allt större utsträckning beroende på riskexponering i förhållande till säkerhetsteknisk mognadsgrad.

Enligt en inventering som SFM genomfört, skiljer sig omfattningen av en cyberförsäkring mellan bolagen till viss del. Följande moment ingår dock som regel i försäkringsskyddet:

- Tillgång till dygnet runt call center för att fastställa om skada föreligger samt koordinering av åtgärder med lämpliga leverantörer

- Ersättning för kostnader:
  - Ersättning för utredningskostnader -vad har inträffat och vad har orsakat incidenten
  - Avbrottsersättning – Förlust av täckningsbidrag om verksamheten begränsas i samband med en cyberincident eller ökade kostnader
  - Ersättning för extrakostnader vid en nätverksincident

- Hjälp vid faktisk eller misstänkt cyberattack exempelvis Ransomware (Förhandling, utredning, hantering, återställande). Endast en försäkringsgivare har tagit principbeslut om att inte ersätta själva lösensumman som sista utväg.

- Ansvarsförsäkring där förlust av personuppgifter, konfidentiell information offentliggörs eller att försäkrad utnyttjas för att exempelvis sprida skadlig programvara till tredje part

- Omvärldsbevakning (tidsbegränsad övervakning av om stulna kort-/personuppgifter används efter intrånget)

3.2 Försäkringsförmedling i Sverige

Försäkringsförmedlare fyller en viktig roll på försäkringsmarknaden och i näringslivet. Försäkringsförmedlare bistår företag med att säkerställa ändamålsenligt försäkringsskydd mot de risker som företagen är exponerade mot samt att dessa risker inte leder till negativ påverkan för det enskilda företaget, näringslivet och samhället i stort.

Den förmedlade sakförsäkringsmarknaden uppgick till cirka 27 miljarder SEK i inbetalda premier under 2021 och växte med 13 % mellan 2020 och 2021. Cirka 800 miljoner SEK av dessa premier är att hänföra till cyberförsäkring som förmedlas i Sverige. Cirka 45 % av förmedlade premier flödar från stora företag, 25 %, kommer från medelstora företag och resterande förmedlade premier kommer från kunder som är småföretag, 18 %, och mikroföretag, 11 %[6].

Försäkringsförmedlarens roll varierar beroende på företagets storlek, kunskap om riskhantering samt organisatorisk komplexitet. Övergripande är försäkringsförmedlarens roll att se över och analysera företagets övergripande försäkringsbehov. Utifrån företaget krav och behov hjälper försäkringsförmedlaren företaget att teckna en lämplig försäkring samt stötta när en skada inträffat.

6 SFM Marknadsrapport: Den förmedlade sakförsäkringsmarknaden i Sverige, 2023.

Försäkringsförmedlare bidrar till försäkringsbolagens produktutveckling genom försäkringsförmedlarens insikt i aktuella marknadsförflyttningar och kundbehov. De har även en viktig roll i att identifiera nya risker och hitta gap i utbudet på försäkringsmarknaden. Försäkringar inom cyber är ett exempel på en sådan utveckling, där förmedlarna drev behovet av att utveckla lösningar för att lösa risker kopplade till cybersäkerhet[7]. Försäkringsförmedlare utgör en viktig part i sin specialiserade roll där slutkunder lätt hamnar i underläge gentemot försäkringsbolagen.

7 National Insurance Brokers Association of Australia (2020).

3.3 Marknadsinsikter från försäkringsbolag – utmaningar och möjligheter

Med stöd av försäkringsbolag och försäkringsförmedlare i SFM:s Forum för Sakförsäkring, har SFM kunnat samla in, och nedan sammanställt, insikter från försäkringsförmedlare och försäkringsbolag inom området för cyberförsäkring.

Många företag är inte försäkringsbara eftersom de inte har en – enligt försäkringskraven – acceptabel skyddsnivå mot cyberhot. Det kan därför vara en tröskel att komma över både vad gäller kostnad och komplexitet att göra rätt saker för att bli försäkringsbar. Vidare ser försäkringsbranschen att införsäkringskrav som sänks i stället leder till undantag eller begränsningar i försäkringsvillkoren.

Det är ändå ett inflöde av försäkringsbolag som vill erbjuda cyberförsäkringar även om flera av dessa börjar med att erbjuda så kallad excessförsäkring, vilket betyder att försäkringsersättningen först blir aktuell vid ett visst skadebelopp.

Den försäkringskapacitet som tidigare fanns i Sverige för cyberrisker har under två års tid begränsats kraftigt. En av anledningarna är att dessa typer av försäkringar är komplexa och kräver mycket kunskap som idag inte finns utbrett på den svenska försäkringsmarknaden. Försäkringsförmedlare som söker cyberskydd för sina kunder, vänder sig då tidvis till mer cybermogna försäkringsmarknader så som London när rätt kapacitet inte återfinns på den svenska försäkringsmarknaden. En annan anledning är att när marknad med så låg penetration snabbt drabbas av stora skador behöver försäkringsgivarna begränsa sin kapacitet för att återfå lönsamhet. En ytterligare insikt är att flera företag missuppfattar omfattningen av cyberförsäkringen. Det framkommer att företagen i många fall har en uppfattning om att cyberförsäkring har en mycket bredare omfattning än vad avsikten är. Ett skäl till detta kan vara okunskap och en begränsad förståelse för grundläggande IT-säkerhet.

Många företag tycker även att cyberförsäkringen är kostsam och i samband med svårighet att förstå försäkringsskyddet bestämmer sig företaget att helt avstå eller väljer en försäkring som inte är anpassad efter behovet.

Utifrån ett försäkringsperspektiv är cyberförsäkring en väsentlig del i ett skydd/IT-säkerhetsperspektiv för företagen. Priset för cyberförsäkring drivs också upp av penetrationen av antalet försäkrade företag. Prisnivån inom cyberförsäkring är och kommer för en tid att vara volatil fram till dess att en mogen marknad uppnås där ett större kollektiv kan bära en normaliserad andel skador, även om nivån det senaste året blivit mer stabil.

3.4 Vad gör försäkringsbolag och försäkringsförmedlare idag och vad kan göras framöver?

Utifrån SFM:s informationsinsamling från försäkringsbolag och försäkringsförmedlare, framkommer att det fortsatta arbetet handlar mycket om samverkan.

Till svenska företag, politiker och samhället i stort, bör det från förmedlar- och försäkringsbranschen handla om att utveckla samarbeten för att sprida kunskap, visa på verkliga skadeexempel och utveckla förutsättningar för gemensam statistik över hur många företag som drabbas inom respektive bransch. Det upplevs även viktigt att försäkringsbolag och/eller försäkringsförmedlare tar fram rapporter med skadeexempel, konsekvenser och förtydligande vad försäkringarna omfattar. Bolagen och förmedlarna bör fortsätta genomföra gemensamma utbildningsinsatser för försäkringsbolag, förmedlare, företag och privatpersoner.
Det går även att ta lärdom av andra länder i utformningen av hanteringen av de digitala hoten. Som jämförelse kan nämnas att Storbritannien som med sina 69 miljoner invånare och NCSC (National Cyber Security Centre) vars budget uppgår till £ 2 miljarder årligen = ca £30 per invånare. Sverige har 10 miljoner invånare och har nationellt cybersäkerhetscenter vars budget är SEK 60 000 000 för 2022 och 2023. Den årlig budgeten är alltså SEK 30 000 000, vilket innebär att per invånare är SEK 3.[8]

Försäkringsförmedlare- och försäkringsbranschen behöver fortsätta lyfta fram fördelarna av bra risk- och krishantering för företagen, vilket även ska inkludera IT och konsekvenser av att inte ha kunskap om sina risker.

Branschen ser avslutningsvis ytterligare möjligheter att samverka med andra privata säkerhetsaktörer, samhällsfunktioner och politiker.

8 Källa: Om centret (ncsc.se)].

Bilaga

Definitioner och begrepp

För finansiella bolag har ett flertal europeiska regelverk beslutats under de senaste åren som rör cyberhot och de risker som bland annat försäkringsbolag kan utsättas för i sin verksamhet. I dessa regelverk har det tagits fram definitioner som kan vara till stöd för förståelse av de begrepp som används i den här rapporten.

Cybersäkerhet:

Bevarande av konfidentialitet, integritet och tillgänglighet vad gäller information och/eller informationssystem via ett cybermedium (internet, sociala medier, bloggar, podcasts etc).

Cyberhot:

En potentiell omständighet, händelse eller handling som kan skada, störa eller på annat negativt sätt påverka nätverks- och informationssystem, användare dessa system och andra personer.

Cyberattack:

Alla former av hackande som leder till ett offensivt/skadligt försök att förstöra, exponera, ändra, deaktivera, stjäla eller få obehörig åtkomst till eller på ett obehörigt sätt använda en informationstillgång som riktar sig mot IT-system.

Cyberincident:

En enskild händelse eller en serie sammankopplade händelser som inte planerats av ett bolag och som äventyrar säkerheten i nätverks- och informationssystemen och har negativ inverkan på tillgängligheten, äktheten, integriteten eller konfidentialiteten vad gäller datan eller de tjänster som tillhandahålls av bolaget. Exempel på incident kan vara:

- Försök att få obehörig åtkomst till ett system/och eller till data.
- Otillåten användning av system för behandling eller lagring av data.
- Ändringar av systemets fasta programvara, mjukvara eller hårdvara utan ägarens medgivande.
- Skadliga avbrott och/eller överbelastning.

Cyberförsäkring:
En försäkringsprodukt som kan se olika ut hos respektive försäkringsbolag, men som normalt innehåller: dygnet runt callcenter för anmälan och identifiering av en incident, återställande av system/data, ersättning för avbrott i företagets verksamhet under incidenten, hantering och notifiering till datasubjekt och myndigheter vid GDPR-incident, ersättning för utredning av skadeståndskrav och juridisk rådgivning vid följer av en cyberincident.

Ransomware:
En metod som hackare använder sig av för att via dataintrång kryptera stora mängder data och begränsa tillgång till system. Därefter begära en lösensumma för att ge tillbaka krypteringsnyckel.

Phishing:
En metod där en aktör, genom att utge sig för att vara någon annan eller företräda ett företag, lurar användare att klicka på länkar eller på annat vis dela med sig av exempelvis inloggningsuppgifter.

MFA:
Multifaktorautentisering, en metod där flera faktorer används för att säkerställa behörighet vid inloggning, exempelvis att via mobiltelefon bekräfta inloggning.

Tryckt av Taberg Media Group i Stockholm 2023. Grafisk form: Spektra design.

Svenska försäkringsförmedlares förening, SFM
Apelbergsgatan 36, 111 37 Stockholm
Telefon 08-545 215 40, info@sfm.se