FSPOS

Finansiella Sektorns Privat-Offentliga Samverkan

Cyberresiliens – vad är det och hur mäts det?

2022-06-13

FSPOS AG Analys

Sammanfattning

Digitaliseringen inom den finansiella sektorn ger nya möjligheter men skapar samtidigt fler risker och en bredare attackyta för antagonistiska aktörer. För att kunna bemöta den nya hotbilden behöver företag tänka i nya banor. Då räcker det inte att enbart förlita sig på traditionella säkerhetsåtgärder som ofta syftar till att upprätta ett starkt skalskydd. Aktörer inom den finansiella sektorn bör därför anamma ett mer holistiskt synsätt kring cyberhot och utgå från att en attack kommer att lyckas. Aktörerna behöver även fokusera på cyberresiliens och förmågan att förutse, motstå, återställa och anpassa sig efter driftsstörningar och cyberattacker.

I denna rapport undersöks begreppet cyberresiliens och hur det kan användas inom den finansiella sektorn. Baserat på enkätfrågor och studier av öppna källor presenteras begreppet enskilt men också i relation till närliggande områden. Rapporten tar även upp exempel på mätpunkter inom cyberresiliens. Rapporten syftar till att ge en nulägesbild av arbetet med cyberresiliens inom den finansiella sektorn, samt bidra till kunskapsspridning avseende verktyg och metoder för mätning inom området.

Introduktion

Den senaste tidens utveckling inom området informationsteknologi har blivit en självklar del av samhället och vardagen, där digitaliseringen erbjuder helt nya möjligheter för människor och organisationer. Men det innebär också nya utmaningar, såväl för samhället i stort som för samhällsviktiga aktörer inom den finansiella sektorn. Riksbankens skriver i sin ekonomiska kommentar *En cyberattack kan påverka den finansiella stabiliteten*[1] att digitaliseringen av finansmarknaden, tillsammans med ökande antal kvalificerade cyberattacker, blottlägger fler sårbarheter hos finansiella aktörer.

För att begränsa dessa sårbarheter blir det systematiska arbetet med identifiering och hantering av cyberrisker allt mer centralt. En cyberrisk karaktäriseras, enligt Riksbanken, av snabbhet och en skalbarhet där konsekvenser snabbt kan få en bred omfattning. En cyberrisk bör därför ses som en systemrisk som kan leda till snabb och stor påverkan på hela det finansiella systemet. Det är således viktigt att verksamheter inom finanssektorn tar höjd för att på något sätt drabbas av exempelvis en cyberattack.

För att säkerställa en god förmåga att hantera cyberattacker, krävs att organisationen aktivt och kontinuerligt arbetar med förbättringar inom cyberområdet. Antal cyberattacker ökar, vilket leder till att *resiliens* blir ett allt viktigare begrepp inom finanssektorn. Cyberresiliens definieras vanligen som förmågan att göra hela organisationen och dess verksamhet motståndskraftig genom att skapa en förmåga att kunna möta, hantera och återhämta sig efter en cyberincident.[2]

Den här rapporten syftar till att ge en nulägesbild av hur den finansiella sektorn ser på och tolkar begreppet cyberresiliens, samt hur sektorn arbetar med verktyg och metoder för mätning inom cyberresiliens. Rapporten riktar sig till personer som på olika sätt arbetar inom finanssektorn med cyberresiliens eller närliggande områden.

Metod

Arbetet med denna rapport inleddes med en kartläggning av olika definitioner av cyberresiliens från relevanta ramverk och standarder inom området. En slutsats av kartläggningen var att cyberresiliens ofta behöver ses i ett sammanhang med närliggande områden. Därför gjordes också en kartläggning av definitioner av områdena cybersäkerhet, informationssäkerhet, organisatorisk resiliens och kontinuitetshantering.

I nästa steg genomfördes en kunskapsinhämtning genom enkätfrågor till utvalda aktörer inom finanssektorn i syfte att undersöka hur de tillfrågade 1) definierar cyberresiliens och 2) arbetar

[1]Riksbanken, 2021, En cyberattack kan påverka den finansiella stabiliteten (riksbank.se)
[2]National Institute of Standards and Technology, 2021, Special Publication 800-160, v2 "*Developing Cyber- Resilient Systems*

med mätning av organisationens cyberresiliens. Frågorna var generellt formulerade för att möjliggöra att cyberresiliens också kan sättas i ett större sammanhang.

Rapporten är ett resultat av både teoretisk datainsamling och praktiska erfarenheter som har samlats in med hjälp av enkätfrågorna och bör läsas som en erfarenhetsdelning mellan aktörer inom den finansiella sektorn. Varje avsnitt inleds med en kort presentation av de erfarenheter som har framkommit i enkätsvaren. Detta följs sedan av en teoretisk ansats som kompletterar erfarenheterna med mer information och fler exempel.

Avgränsningar

Datainsamling i form av enkätfrågor har koncentrerats på inhämtning av erfarenheter från sektorns arbete inom området cyberresiliens. Rapporten avser inte att på något sätt utvärdera eller mäta mognaden av sektorns förmåga inom cyberresiliens.

De erfarenheter som presenteras i rapporten ska ses som exempel på hur organisationer inom finanssektorn kan arbeta med mätning inom cyberresiliens. Rapporten gör inte anspråk på att redovisa en fullständig bild.

Cyberresiliens – vad är det?

Det finns idag ingen entydig definition av begreppet cyberresiliens, men olika beskrivningar är vanligt förekommande i ramverk och standarder inom området. Det är vanligt att dessa innehåller övergripande målsättningar, underliggande mål och ibland även metoder för att uppnå cyberresiliens.

Enligt öppna källor använder flera aktörer National Institute of Standards and Technology (NIST) Special Publication 800-160, v2 *"Developing Cyber- Resilient Systems"* i sitt arbete med cyberresiliens.[3]

I beskrivningen av cyberresiliens utgår NIST från att en incident inträffar som medför negativa konsekvenser för den drabbade organisationen, snarare än att enbart fokusera på att incidenter inte får inträffa. Vidare beskriver NIST att cyberresiliens avser organisationens förmåga att kunna förutse, motstå, återställa och anpassa *(eng: Anticipate, Withstand, Recover and Adapt)* under svåra förhållanden, påfrestningar och attacker mot system som använder eller är beroende av cyberresurser.[4] Definitionen kan exempelvis tillämpas på ett system, en komponent, en tjänst eller ett geografiskt avgränsat område.

Figur 1. Figuren beskriver NIST SP 800 - 160 definition av cyberresiliens.

Olika förmågor inom cyberresiliens

Förmågan att kunna förutse avser att undvika, avskräcka och förhindra eventuella hot, och omfattar även planering, identifiering av resurser samt att skapa planer för hur resurserna ska användas när ett hot uppstår. Ett exempel kan vara att förändra tillgängliga resurser eller system för att minimera attackytan och därigenom göra det svårare för en antagonistisk aktör att uppfylla sina mål.

Förmågan att kunna motstå avser att acceptera en viss nivå av skada eller påverkan på delar av ett system, samt att vidta åtgärder för att reducera påverkan på andra delar av systemet och automatiskt reparera skadan. Det kan även innebära att överföra händelser eller effekten av händelser till andra delar av ett system, samt att byta ut eller göra sig av med system som kan ha påverkats.

[3] Financial Stability Board, 2018, Cyber Lexicon - Financial Stability Board (fsb.org)
[4] National Institute of Standards and Technology, 2021, Special Publication 800-160, v2 *"Developing Cyber- Resilient Systems*

Förmågan att kunna återställa avser att ett system återgår till ett tidigare, fungerande läge exempelvis baserat på befintliga säkerhetskopior. Utifrån dessa kan systemet återfå kritiska funktioner till acceptabla nivåer, alternativt använda tillgängliga alternativa systemresurser. Övriga strategier är att byta ut system som indikerar skada.

Förmågan att kunna anpassa omfattar flertalet strategier som exempelvis härdning. Med detta avses att minska eller förändra attackytan vid en cyberincident, till exempel genom att begränsa antalet applikationer i it-miljön. En annan strategi är korrigering *(eng: correction)*, vilket innebär att organisationen bör lägga till eller ta bort kontroller för att kompensera för upptäckta sårbarheter. Ett exempel på korrigering är upptäckten av en kritisk sårbarhet i organisationens lösning för multifaktorautentisering, vilket kräver att den tas bort och ersätts med en utökad policy för lösenord. Vidare kan en organisation omorientera, vilket avser att proaktivt arbeta med kontroller, processer och förmågor alltefter hotlandskapets utveckling. Dessa strategier kan resultera i en förändring av systemets arkitektur och design, men även operativa processer.

NIST som utgångspunkt

NISTs definition av cyberresiliens återspeglas i såväl enkätsvar som i andra ramverk och standarder. I tabellen nedan framgår att exempelvis *Financial Stability Board* i sitt cyberlexikon har definierat begreppet cyberresiliens med utgångspunkt i samma nyckelord som återfinns i NIST. Det som utmärker denna definition är att ordet ”organisation” används, vilket kan tänkas möjliggöra en bredare tolkning av begreppet.[5] Av enkätsvaren framkommer också ett tydligt mönster att många aktörer i den finansiella sektorn använder definitioner av cyberresiliens som är snarlika med NIST.

I tabellen nedan presenteras ytterligare ett exempel på definition från boken *Cyber Resilience of Systems and Networks*[6]. Även denna definition är snarlik med NIST, främst tack vare användandet av snarlika nyckelord. Skillnaden är dock att denna definition är något mer tekniskt orienterad genom dess tydliga formulering att cyberresiliens är direkt kopplat till en cyberattack.

NIST	Financial Stability Board	Cyber Resilience of Systems and Networks
The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment.	The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents.	The ability of the system to prepare, absorb, recover, and adapt to adverse effects, especially those associated with cyberattack.

Tabell 1. Olika definitioner av begreppet cyberresiliens.

[5] T.ex. Financial Stability Board, 2018, Cyber Lexicon - Financial Stability Board (fsb.org)
[6] Alexander Kott & Igor Linkov, 2019

Cyberresiliens i relation till närliggande områden

Av enkätsvaren framgår att cyberresiliens som begrepp sällan är tydligt definierat hos aktörer i den finansiella sektorn. Däremot har samtliga aktörer som besvarat enkäten gjort en bedömning att de har processer som helt eller delvis omfattar begreppet cyberresiliens. Områden som är relaterade till cyberresiliens är informationssäkerhet och cybersäkerhet, kontinuitetshantering, organisatorisk resiliens *(eng: operational resilience)* och digital operativ motståndståndskraft.

Informationssäkerhet och cybersäkerhet

Områdena informationssäkerhet och cybersäkerhet är nära förknippade med cyberresiliens. Cyberresiliens, enligt NISTs definition, har fokus på en förmåga att snabbt kunna återhämta sig efter en händelse. Därav utgår definitionen från antagandet att ett system har påverkats negativt, vilket sätter fokus på ständiga förbättringar av förebyggande och mildrande åtgärder. Området cybersäkerhet utgår från ett delvis annorlunda antagande. Här är fokus på säkerhetsåtgärder för att förhindra, upptäcka och agera mot cyberangrepp. Centralt inom cybersäkerhet är en strävan att skydda konfidentialitet, riktighet och tillgänglighet av digitaliserad information. Detta uppnås genom att skydda elektroniska system med tekniska, administrativa och kulturella åtgärder.[7]

Området informationssäkerhet syftar likt cybersäkerhet till att skydda konfidentialitet, riktighet och tillgänglighet av information, med skillnaden att det även innefattar alla former av analog information. NIST definierar informationssäkerhet enligt *"The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."*[8] Både informationssäkerhet och cybersäkerhet beskriver åtgärder för att minska risken för informationssäkerhetsincidenter, medan cyberresiliens även hanterar konsekvenserna av cyberrisker.

Kontinuitetshantering

Ytterligare ett begrepp som knyter an till området cyberresiliens är kontinuitetshantering. FSPOS definierar kontinuitetshantering som den process som skapar en robusthet i organisationen i syfte att bättre kunna hantera förluster av delar av, eller hela, den operativa förmågan och därigenom skyddar organisationens intressenter, rykte, varumärke och värdeskapande aktiviteter.[9] Även här finns en tydlig koppling till cyberresiliens genom fokus på upprätthållande av verksamhet oavsett orsaken till störning eller avbrott.

Organisatorisk resiliens

Begreppet cyberresiliens kan även tillämpas i den bredare kontexten av organisatorisk resiliens *(eng: operational resilience)*. FSPOS beskriver organisatorisk resiliens som "resultatet av ett integrerat beredskapsarbete som sträcker sig över samtliga berörda beredskapsdiscipliner och

[7] Läs mer på Informationssäkerhet.se- Stöd för systematiskt arbete med informationssäkerhet i organisationer
[8] National Institute of Standards and Technology, Glossary information Security
[9] FSPOS, 2021, Vägledning för kontinuitetshantering

genomsyrar hela organisationen, där ägandeskapet på ett tydligt sätt ligger på ledningsnivå".[10] Cyberresiliens utgör tillsammans med flertalet andra discipliner viktiga beståndsdelar i det integrerade beredskapsarbete som syftar till organisatorisk resiliens.

Digital operativ motståndskraft

Ett ytterligare närbesläktat begrepp till cyberresiliens är digital operativ motståndskraft *(eng: digital operational resilience)* som beskrivs i *Digital Operational Resilience Act (DORA)*.[11] Kort beskrivet syftar DORA till att stärka den finansiella sektorns motståndskraft mot cyberrisker genom att vidta relevanta skyddsåtgärder för att motverka bland annat cyberattacker.[12] DORA definierar digital operativ motståndskraft som "*The ability of a financial entity to build, assure and review its operational integrity from a technological perspective by ensuring, either directly or indirectly, through the use of services of ICT third-party providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity makes use of, and which support the continued provision of financial services and their quality*". [13]

Digital operativ motståndskraft har tydliga likheter med cyberresiliens. Vid en första anblick ligger båda dessa definitioner i linje med varandra (se NISTs definition av cyberresiliens i tabell 1) då båda söker motverka konsekvenserna vid inträffade cyberhändelser. DORA har dock en tydligare definierad målsättning då den specifikt innefattar upprätthållandet av finansiella tjänster och deras kvalitet. NIST specificerar däremot inte målsättningen utan konstaterar att uppdrag och affärsmål, som är beroende av cyberresurser, ska kunna uppnås i en it-miljö där kontroll eller användning av resurser kan vara otydlig.

Sammanfattning

Gemensamt för cyberresiliens och för ovan redogjorda begrepp är att de på olika sätt syftar till att minska konsekvenserna och/eller sannolikheten för cyberrisker. Givet hotbilden och dagens komplexa it-miljöer krävs en medveten strategi och ett arbetssätt baserat på inte bara ett utan flertalet begrepp och områden som kompletterar varandra. Därigenom kan en ännu högre grad av resiliens uppnås i organisationen.

Mätningar, varför och hur?

Betydelsen av cyberresiliens har ökat och därigenom företagsstyrelsernas intresse för olika mätpunkter och nyckeltal. För att på ett effektivt sätt kunna följa upp arbetet med cyberresiliens, kan en organisation använda sig av olika verktyg och metoder för att mäta sin förmåga inom området. Generellt finns olika svårigheter inom mätning av cyberresiliens. Ofta är mätpunkter

[10] FSPOS, 2021, PM Organisatorisk Resiliens.pdf
[11] Översättning från Regeringskansliet, se Förordning om digital operativ motståndskraft i den finansiella sektorn
[12] Sveriges riksdag, 2020, Förordning om digital operativ motståndskraft i den finansiella sektorn
[13] Europeiska kommissionen, 2018, Regulation of the European parliament and of the council

tekniska, eller träffar inte rätt med avseende på *effekten* av arbetet med cyberresiliens. En ytterligare viktig aspekt är betydelsen av att göra mätpunkter *begripliga* för företagsstyrelsen eller andra beslutsfattare. Därför är valet av *relevanta* mätpunkter och nyckeltal en avgörande faktor för att uppnå målen med cyberresiliens i organisationen.

Av enkätsvaren framgår att det finns många olika anledningar till varför aktörerna genomför mätningar. Det handlar dels om krav från företagsstyrelser, ledningsgrupper och kunder, dels att uppnå efterlevnad av regulatoriska krav och certifieringskrav. En aktör lyfter fram mätning som en viktig del i att identifiera gap mellan befintlig och önskad nivå i syfte att kunna implementera relevanta kontroller utifrån resultatet. Majoriteten av aktörerna är eniga om att huvudsyftet med mätningar inom cyberresiliens är att möjliggöra för väl avvägda, riskbaserade prioriteringsbeslut.

Exempel på mätpunkter

Flertalet aktörer genomför olika former av mätningar och uppföljningar som i någon grad inkluderar cyberresiliens. Dessa mätningar har främst koppling till informationssäkerhet och cybersäkerhet. Några exempel på både kvalitativa och kvantitativa mätpunkter som anges är:

- Procentuell andel av Endpoint Detection and Response[14] (EDR) på organisationens endpoints
- Antal kända sårbarheter per tjänst eller funktion
- Procentuell andel anställda och konsulter som har genomgått säkerhetsutbildning

Användning av både kvalitativa och kvantitativa mätpunkter är viktiga instrument för att dels mäta organisationens mognadsgrad inom cyberresiliens[15], dels öka möjligheten att snabbt kunna upptäcka avvikelser i systemens prestanda. I tabell 2 nedan anges ytterligare exempel på kvalitativa och kvantitativa mätpunkter som ett komplement till det som framkommit i enkätsvaren.

[14] Teknik för kontinuerlig övervakning av enheter (t.ex. servrar, bärbara datorer och mobiler) för att identifiera, varna och automatiskt genomföra åtgärder för att skydda mot antagonistiska cyberhot. Detta sker med hjälp av korrelation av data från flera olika källor.
[15] Metod för en strukturerad mätning över tid med syfte att redovisa utvecklingen av cyberresiliens.

Exempel på kvalitativa mätpunkter
• *Fungerar våra processer för backuphantering i händelse av en incident?* • *Har beslutsfattare inom organisationen tillgång till den informationen de behöver för att kunna fatta kritiska beslut före, under och efter en incident?* • *Är utbildning av personal utformad för att hantera relevanta incidenter?* • *Hur fungerar processen för utvärdering av cyberhändelser?* • *Hur bidrog CCoA (Cyber Course of Action)[16] vid incident till att upprätthålla finansiella tjänsters konfidentialitet, riktighet och tillgänglighet?*
Exempel på kvantitativa mätpunkter
• *MTTR Mean Time To Resolve* (genomsnittlig tid för att ”lösa” en incident) • *TTR Time To Recovery* (tid för återställning av system) • *MDT Mean Down Time* (genomsnittlig tid som ett system är nere) • *Web server requests per second* (förmåga att hantera HTTP requests) • *Procent av användare med administratör eller privilegierade rättigheter*

Tabell 2. Exempel på kvalitativa och kvantitativa mätpunkter.

För att uppnå en hög mognadsgrad inom cyberresiliens behöver ett flertal faktorer beaktas. En viktig utgångspunkt är samspelet mellan människor, process och teknik *(eng: people, process and technology)*. Samtliga tre aspekter behöver beaktas vid urvalet av kvalitativa och kvantitativa mätpunkter. Likaså är urvalet av relevanta mätpunkter inom cyberresiliens mycket stort. I rapporten *”Cyber Resiliency Metrics Catalog”*[17] anges nära 500 exempel på mätpunkter kopplade till olika mål för organisationens mognad.

Oavsett hur en organisation väljer att mäta mognad inom cyberresiliens är det viktigt att anpassa mätningarna utifrån organisationens mål, strategi och förutsättningar. Därutöver behöver mätningar inom cyberresiliens vara en integrerad del i organisationens riskhanteringsarbete för att kunna besluta om rätt och effektiva åtgärder vid avvikelser. I enkätsvaren belyser flertalet aktörer vikten av att utgå från organisationens befintliga ramverk för mätningar. Därigenom kan nya mätpunkter läggas till inom ramen för ständiga förbättringar.

Olika sätt att arbeta med och mäta cyberresiliens

I enkätsvaren anges ett flertal exempel på olika ramverk, standarder och verktyg som är till stöd i arbetet med cyberresiliens. I tabell 3 nedan presenteras några av dessa exempel och hur de relaterar till mätning inom cyberresiliens. Genom att kombinera flera ramverk, standarder och verktyg kan organisationen erhålla ett bredare spektrum av relevanta mätpunkter och nyckeltal.

[16] En sekvens av införda riskhanteringsåtgärder för att möta cyberincidenter.
[17] The mitre Corporation 2018, Cyber Resiliency Metrics Catalog

Ramverk/standard/ verktyg	Kort beskrivning	Relation till mätning av cyberresiliens
ISO 27001	ISO 27001 är en standard som avser att ge stöd till det systematiska arbetet med informationssäkerhet.	Standarden kan tillämpas genom att mäta effektiviteten hos de säkerhetsåtgärder som en aktör väljer att införa. En aktör kan även välja mätpunkter med koppling till processer till ledningssystemet för informationssäkerhet, exempelvis incidenthanteringsprocessen. En relevant mätpunkt i detta fall är genomsnittstiden för att lösa en incident.
ISO 22301	ISO 22301 är en standard för kontinuitetshantering. Standarden belyser krav för att planera, upprätta, införa, tillämpa, övervaka, underhålla och ständigt förbättra för att skydda mot, minska sannolikheten, förbereda för, agera på och återställa organisationens förmåga vid avbrott.	Standarden kan användas som utgångspunkt för aktörers arbete med kontinuitetshantering och kan därigenom även utgöra en grund för vilka parametrar som behöver mätas för att säkerställa kontinuitet inom väsentliga processer. Standarden redogör inga exempel på mätpunkter men beskriver övergripande nyttan med revisionsprogram, vikten av kvantitativa och kvalitativa mått, samt användningen av ledningens genomgång som ett forum för ständig förbättring.
NIST Cyber Security Framwork	NIST har publicerat ramverket *"Framework for Improving Critical Infrastructure Cybersecurity"* (NIST CSF).[18] Detta ramverk syftar till att ge organisationer vägledning inom området cybersäkerhet. Här definieras fem kärnfunktioner som kan användas som utgångspunkt i arbetet med cybersäkerhet; *identify, protect, detect, respond, recover*.	Ramverket specificerar inte några mätpunkter annat än de kontroller som kan innefattas i de ramverk och standarder som ramverket refererar till. NIST CSF nämner vikten av att vara noggrann med vilka mätpunkter som används och uppmuntrar till att analysera varför specifika mätpunkter ska användas för att undvika missvisande resultat och därav få en falsk bild av hanteringen av cyberrisker.
Cyber Risk Institute Profile (CRI profile)	*The Cyber Risk Institute* (CRI) tillhandahåller ett verktyg för mätning av en organisations arbete med cyberrisker.[19] Verktyget, CRI Profile, är baserat på NIST CSF men är kompletterat med två ytterligare kärnfunktioner; *Governance* och *Supply chain management*. Denna komplettering syftar till att fånga upp och omhänderta krav på aktörer inom den finansiella sektorn. Några exempel är krav från *Committee on Payments and Market Infrastructures* och *International Organization of Securities Commissions* (CPMI-IOSCO).	Profile-verktyget kan användas konkret vid mätning för bedömning av effektnivå i kärnfunktioner. Bedömningen av effektnivå möjliggör utvärdering av arbetet med cyberresiliens. Verktyget föreslår att resultatet av utvärderingen används till genomförandet av en gap-analys. Gap-analysen mynnar i sin tur ut i en handlingsplan där aktören kan hantera identifierade gap och risker med hjälp av de ramverk och standarder som Profile refererar till.

[18] National Institute of Standards and Technology, 2018, Cyber Security Framework
[19] Cyber Risk Institute, 2022, The profile

Center of Information Security	*Center of Internet Security* (CIS) är en organisation som tillhandahåller kontroller och mätpunkter inom främst it-säkerhet. [20]	CIS består av 18 kontrollområden, med ett antal kontroller under respektive område, som används för att hantera cyberrisker. Kontrollerna är uppdelade i olika grupper som möjliggör för en organisation att utifrån riskanalys och tillgängliga resurser välja ut en adekvat nivå för riskhantering. CIS ger även mätpunkter för uppföljning av implementationsprojekt CIS tillhandahåller även konfigurationsguider som representerar *best practice* inom härdning av olika hård- och mjukvaror som är vanligt förekommande hos företag. Med hjälp av automatiserade verktyg kan en aktör analysera efterlevnaden av härdning enligt konfigurationsguider för respektive komponent.
DORA	Förordningen om *Digital Operational Resilience Act* (DORA) syftar till att stärka den finansiella sektorns motståndskraft mot cyberrisker genom att vidta relevanta skyddsåtgärder för att motverka bland annat cyberattacker. DORA innehåller krav som syftar till att aktörer aktivt ska arbeta för att bli mer motståndskraftiga mot informations- och kommunikationsrelaterade (IKT) störningar och hot. [21]	Mätpunkter kan utformas utifrån krav beskrivna i DORA. Exempelvis nämns *Recovery Time Objectives* (RTO) som relaterar till kvantitativ mätning av digital operativ motståndskraft. Genom att uppnå en kortare *Time To Recovery* (TTR) efter en negativ händelse, utan att äventyra konfidentialiteten eller riktigheten i information, kan en organisation betraktas som mer resilient.

Tabell 3. Exempel från enkätsvar på ramverk och verktyg aktörer kan använda sig utav inom området cyberresiliens.

Avslutande reflektioner

Cyberresiliens bygger på metoder för att hantera aktörernas förmåga att kunna förutse, motstå, återställa och anpassa vid cyberhot. En aktör behöver ha ett robust och heltäckande ramverk för cyberresiliens för att styra och hantera cyberhot. Arbetet med rapporten har visat att det finns både utmaningar och möjligheter i det viktiga arbetet med cyberresiliens.

En utmaning ligger i begreppets definition. Idag är begreppet inte exakt definierat och inom finanssektorn används det än så länge i begränsad omfattning. De tillämpningar som finns inom sektorn tar helt eller delvis sin utgångspunkt i NIST. För att möta ett växande behov inom sektorn, i kombination med nya regulatoriska krav inom området, behöver aktörerna förstå och tolka innebörden av begreppet cyberresiliens för att därigenom kunna bygga förmåga.

Förståelsen av att cyberresiliens är en del i ett större sammanhang är nödvändig men medför också utmaningar. Cyberresiliens delar många processer och åtgärder med närliggande områden. Detta ställer krav på att arbetet med cyberresiliens harmoniserar med organisationens

[20] Center of Information Security, 2022, CIS
[21] Sveriges riksdag, 2020, Förordning om digital operativ motståndskraft i den finansiella sektorn

övriga arbete med exempelvis informationssäkerhet, kontinuitetshantering, riskhantering och compliance.

Arbetet med cyberresiliens medför även nya möjligheter. När begreppet är definierat och dess relation till närliggande områden är känt, kan organisationen följa upp och kontinuerligt förbättra arbetet med cyberresiliens. Detta möjliggörs genom en kombination av kvalitativa och kvantitativa mätpunkter och nyckeltal som är begripliga och relevanta. Därigenom skapas goda möjligheter för en aktör att möta utmaningarna i en allt mer digitaliserad verksamhet, och samtidigt kunna tillmötesgå nya regulatoriska krav på sektorns arbete med hantering av cyberrisker.