

Från informationssäkerhet till cybersäkerhet

– samhällsekonomiska konsekvenser av en begreppsförskjutning

DANIELA ANDRÉN, FREDRIK KARLSSON OCH ROSE-MHARIE ÅHLFELDT

Inom informationssäkerhetsområdet har en tydlig begreppsförskjutning skett under de senaste två decennierna. EU:s strategidokument (European Commission 2020; European Union 2022; European Union 2024) och svensk lagstiftning och myndighetskommunikation (Myndigheten för samhällsskydd och beredskap) (MSB 2024a; MSB 2024b) använder numera cybersäkerhet som huvudbegrepp. Det bredare begreppet informationssäkerhet trängs undan eller behandlas synonymt med det snävare begreppet cybersäkerhet.

Ur ett nationalekonomiskt perspektiv är denna förändring inte neutral: den förändrar hur aktörer definierar problem, fördelar resurser och fattar investeringsbeslut. När informationssäkerhet reduceras till en teknisk fråga (även om detta inte alltid är den ursprungliga avsikten med begreppsförskjutningen) förändras den ekonomiska incitamentsstrukturen och ansvarsfördelningen på ett sätt som kan förvärra redan välkända marknadsimperfectioner. Problemet är alltså inte enbart vilket ord som används, utan vilka typer av risker som prioriteras. När fokus ligger på cybersäkerhet tenderar tekniskt synliga risker att prioriteras framför organisatoriska och mänskliga risker. Lantmäteriets säkerhetsincident 2024 (Carlsson 2024) är ett illustrativt exempel: det var brister i det organisatoriska säkerhetsarbetet snarare än rent tekniska fel som stod i centrum. Fallet illustrerar att ansvaret för informationssäkerheten inte var förankrat på

strategisk nivå. Denna artikel belyser tre ekonomiska mekanismer genom vilka begreppsförskjutningen kan påverka resursallokering och samhällsekonomisk effektivitet och diskuterar de policyimplikationer som följer.

Begreppens ekonomiska innebörd

Enligt ISO 27000 (ISO 2018), en internationell standard för informationssäkerhet, omfattar informationssäkerhet skydd av information i alla digitala och analoga former och integrerar tekniska, administrativa och organisatoriska perspektiv. Cybersäkerhet fokuserar på skydd mot cyberrisker och utgör en delmängd av det bredare begreppet informationssäkerhet (ISO 2024).

Distinktionen är ekonomiskt viktig eftersom den påverkar hur säkerhetsarbetet organiseras, vad som kan mätas och vem som hålls ansvarig. Informationssäkerhet i vid bemärkelse är en *integrerad funktion* som kräver investeringar i teknologi, organisation och humankapital som tillsammans bidrar till säkerheten. När cybersäkerhet blir det dominerande styrningsbegreppet riskerar säkerhetsarbetet att behandlas som en *avgränsad teknisk funktion* som delegeras till IT-avdelningar. Organisationer som gör detta tenderar att uppvisa en mindre effektiv säkerhet och kan få högre totalkostnader på grund av suboptimal resursallokering (IBM Security 2024). Branschrapporter pekar på att organisatoriska och mänskliga faktorer ofta har varit avgörande vid säkerhetsincidenter (t ex ENISA 2024).

Den nationalekonomiska forskningen om informationssäkerhet etablerades som ett distinkt forskningsfält omkring år 2000. En central iakttagelse är att informationssäkerhetsbrister ofta uppstår när ekonomiska incitament, ansvar och riskbärande inte sammanfaller, och att sårbarheten ökar särskilt när den aktör som ansvarar för skyddet inte är densamma som bär kostnaderna vid misslyckan-

INLÄGG

Daniela Andrén är universitetslektor i nationalekonomi vid Örebro universitet och docent i nationalekonomi vid Göteborgs universitet. Hennes forskningsintressen är arbetsmarknadsekonomi och välfärdsekonomi, kausal inferens och etiska aspekter av algoritmer. daniela.andren@oru.se

Fredrik Karlsson är professor i informatik vid Örebro universitet. Hans forskning rör ledning och styrning av informationssäkerhet, agila systemutvecklingspraktiker samt digitalisering i organisationer. fredrik.karlsson@oru.se

Rose-Mharie Åhlfeldt är professor i informationsteknologi vid Högskolan i Skövde. Hennes forskning rör informationssäkerhet, cybersäkerhet, integritetsskydd och digital transformation. rose-mharie.ahlfeldt@his.se

den (Anderson och Moore 2006). Mot denna bakgrund belyses tre ekonomiska mekanismer som kan förstärka problemen med begreppsförskjutningen.

Tre ekonomiska mekanismer

Begreppsförskjutningen gör vissa risker – särskilt tekniska risker – mer synliga, medan organisatoriska och mänskliga risker får mindre uppmärksamhet. Vi belyser här tre centrala ekonomiska mekanismer genom vilka begreppsförskjutningen kan påverka resursallokering och samhällsekonomisk effektivitet: 1) snedvridna investeringsbeslut, 2) förstärkta externaliteter och 3) asymmetrisk information på mjukvarumarknaden. Dessa mekanismer hänger nära samman, men kan analytiskt särskiljas för att tydliggöra hur incitament och beslut påverkas.

Den första mekanismen tar sin utgångspunkt i den rigorösa ekonomiska modellen för optimal säkerhetsinvestering som Gordon och Loeb (2002) presenterat. Modellen visar, under sina antaganden om hur säkerhetsutgifter påverkar sannolikheten för intrång, att den optimala investeringen inte bör överstiga 37 procent ($1/e$) av den förväntade förlusten från ett säkerhetsintrång. Ett viktigt resultat från modellen är att den högsta ekonomiska avkastningen ofta uppnås genom att prioritera informationstillgångar med medelhög sårbarhet snarare än de allra mest sårbara. Modellen förutsätter dock också att beslutsfattare har en tillräckligt heltäckande bild av organisationens informationstillgångar, sårbarheter och förväntade förluster.

Begreppsförskjutningen mot cybersäkerhet kan undergräva denna förutsättning på två sätt. För det första kan beslutsfattare underskatta de totala möjliga förlusterna om icke-digitala informationstillgångar lämnas utanför när organisatoriska och mänskliga faktorer förbises i sårbarhetsbedömningarna. Resurser kan då läggas på digitala

tillgångar med hög synlig risk, medan tillgångar med medelhög risk, som ofta rör organisatoriska eller mänskliga säkerhetsdimensioner, förbises. Denna allokering är suboptimal enligt modellen. För det andra kan beslutsprocessen splittras när cybersäkerhet delegeras till IT-avdelningar. Därmed förskjuts investeringar mot det som är lätt att observera, mäta och rapportera, inte nödvändigtvis mot det som ger störst nytta för samhället eller för organisationens egen marginalavkastning.

Den andra mekanismen handlar om att informationssäkerhet karaktäriseras av omfattande externaliteter. En aktörs förbättringar av säkerheten minskar risken att aktörens system används för attacker mot andra – en positiv externalitet. Ömsesidigt beroende risker skapar ett klassiskt kollektivt handlingsproblem: rationella aktörer väljer en lägre säkerhetsnivå än vad som är socialt optimalt och *free-riding* uppstår (Kunreuther och Heal 2003). Gordon m fl (2015) visar att den socialt optimala investeringen ökar med högst 37 procent ($1/e$) av den förväntade externalitetsförlusten när externaliteter inkluderas i kalkylen, vilket innebär att enskilda aktörer investerar mindre än vad som är bäst för samhället.

Om fokus ligger på tekniska risker i den egna organisationen blir det lätt att bortse från organisatoriska åtgärder som minskar risker för andra områden, t ex i leverantörskedjor. Exempelvis kan brister i utbildning, åtkomsthantering, leverantörsstyrning eller säkerhetskultur exponera andra organisationer via gemensamma tjänster, leveranskedjor och delade plattformar, utan att den enskilda aktören fullt ut bär kostnaderna. Resultatet kan bli att organisationer investerar för lite i säkerhet ur ett samhällsperspektiv. Åtgärder som också skyddar andra aktörer prioriteras bort, särskilt när de är svåra att mäta och följa upp internt.

Den tredje mekanismen handlar om

att mjukvarumarknaden präglas av betydande asymmetrisk information mellan säljare och köpare. Leverantörer gör påståenden om produkters säkerhet, men köpare saknar möjlighet att verifiera dessa, och i många fall känner inte ens leverantören till den faktiska säkerhetsnivån. Detta skapar en klassisk marknad för *lemons* (Akerlof 1970): när köpare inte kan skilja säker från osäker mjukvara har leverantörer av säkrare produkter svårt att erhålla högre priser, vilket systematiskt försvagar incitamenten att investera i säkerhet (Anderson och Moore 2006). Konsumenter belönar i stället funktioner, snabb marknads lansering och marknadsdominans – incitament som förstärks av nätverksexternaliteter på plattformsmarknader (Katz och Shapiro 1985). Nätverkseffekter driver dessutom teknologisk inlåsning: när en plattform uppnått en tillräckligt stark ställning på marknaden blir alternativa, potentiellt säkrare lösningar svåra att etablera även om de vore överlägsna (Arthur 1989).

Begreppsförskjutningen kan koncentrera köparnas uppmärksamhet på lättobserverade tekniska och ofta checklistbaserade säkerhetsfunktioner som t ex brandväggar och kryptering, medan svårkontrollerade säkerhetsegenskaper kopplade till systemens utformning, arbetsflöden och möjliga integrationer i organisationen nedprioriteras av både säljare och köpare. Dataläckan hos Miljödata, där flera organisationer delade samma molntjänst och drabbades tillsammans (Sjödin 2025), illustrerar hur nätverkseffekter och asymmetrisk information kan samverka när beroendet av leverantörer samlar risker till ett fåtal gemensamma IT-miljöer. Fallet är illustrativt snarare än bevisande, men det ligger väl i linje med den ekonomiska teorin.

Konsekvenser och åtgärder

De beskrivna mekanismerna medför konkreta samhällsekonomiska conse-

kvenser. Organisationer riskerar att lägga för mycket pengar på tekniska lösningar som ger liten extra säkerhet, samtidigt som investeringar i organisatoriska åtgärder och humankapital undervärderas. Samtidigt kvarstår systematisk underinvestering i åtgärder vars nytta till betydande del tillfaller andra aktörer. Transaktionskostnaderna ökar när koordination försvåras av splittrat ansvar.

Medierapporteringen fokuserar ofta på spektakulära cyberattacker (t ex *Dagens Nyheter* 2024) medan mänskliga och organisatoriska aspekter hamnar i skymundan. Att Lantmäteriet, i det inledande exemplet, inte hade förankrat sin informationssäkerhet, ledde till fragmenterade incitament och suboptimal riskhantering. Svenska incidenter visar därmed hur organisatoriska, tekniska och mänskliga aspekter samverkar. De illustrerar inte i sig ett kausalt samband, men de är förenliga med artikelns teoretiska mekanismer.

Detta överensstämmer med vad den ekonomiska teorin förutsäger när säkerhetsansvar fragmenteras, inte förankras på strategisk nivå och/eller delegeras utan en tydlig incitamentsstruktur. Lagstiftningen utformas med cybersäkerhet i fokus, vilket riskerar att bredare säkerhetsaspekter inte regleras adekvat (SOU 2024:18). Forskningsfinansiering koncentreras till tekniska cybersäkerhetsprojekt medan forskning om mänskliga, organisatoriska och ekonomiska aspekter marginaliseras.

Tre policyåtgärder framstår därför som centrala. För det första bör informationssäkerhet återetableras som det övergripande begreppet i regelverk, lagstiftning och forskningsfinansiering för att motverka att resurser felfördelas när syftet är styrning av organisationers samlade riskhantering. Cybersäkerhetens specifika utmaningar ska inte förbises utan integreras i en bredare kontext. Vid implementeringen av exempelvis

NIS2 (EU-regelverket som ställer krav på cybersäkerhet, riskhantering och incidentrapportering för samhällsviktiga och digitala verksamheter) bör det tydligt framgå att lagkraven ingår i organisationens systematiska informationssäkerhetsarbete och inte utgör ett separat tekniskt stuprör. På så sätt skapas förutsättningar för mer heltäckande riskvärdering, bättre prioritering och högre ekonomisk effektivitet.

För det andra krävs mekanismer för att ta hänsyn till externaliteter: differentierade krav, kostnader kopplade till risker, upphandlingskrav som adresserar leverantörskedjor, och otydligt ansvar för aktörer med systembärande roller (Kunreuther och Heal 2003; Gordon m fl 2015). Obligatorisk incidentrapportering, som NIS2 inför för samhällskritiska sektorer, är ett steg i rätt riktning. Effekten begränsas dock om rapporteringen sker med ett snävt tekniskt fokus som inte fångar upp organisatoriska och mänskliga faktorer.

För det tredje bör nationella satsningar som t ex Cybercampus Sverige och forskningsfinansiärer som t ex Myndigheten för civilt försvar (MCF, tidigare MSB), Nationellt cybersäkerhetscenter (NCSC), Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet (NCC-SE) och Vetenskapsrådet aktivt bredda sina program bortom tekniska perspektiv. Sådan forskning har karaktären av en kollektiv nytthet vars samhälleliga avkastning överstiger den privata, vilket gör att offentlig finansiering behövs för att motverka att det annars forskas för lite om dessa aspekter. Forskning om incitamentsstrukturer, organisatoriska säkerhetspraktiker, upphandling och ekonomiska aspekter av säkerhet är nödvändig för att minska problemen med asymmetrisk information och förbättra möjligheten att specificera och kontrollera säkerhetsprestanda i avtal och uppföljning. Standardisering och certi-

fiering enligt den internationella ISO 27000-serien kan också minska problemen med asymmetrisk information på marknaden (Akerlof 1970) genom att öka jämförbarhet och verifierbarhet (ISO 2022).

Slutsatser

Begreppsförskjutningen från informationssäkerhet till cybersäkerhet ändrar de ekonomiska villkoren för hur säkerhet definieras, mäts och styrs: från en integrerad funktion som kräver investeringar i teknologi, organisation och humankapital, till en teknisk funktion som riskerar att hanteras separat. När cybersäkerhet blir huvudfokus kan organisationer komma att prioritera det som är lätt att mäta snarare än det som faktiskt minskar riskerna mest. Denna förskjutning kan förvärpa välkända marknadsimperfectioner längs tre ekonomiska mekanismer: 1) optimal investering enligt Gordon-Loeb-modellen försvåras när beslutsfattare saknar helhetsperspektiv; 2) externaliteter leder till systematisk underinvestering när mänskliga och organisatoriska aspekter osynliggörs; och 3) problemen med asymmetrisk information på mjukvarumarknaden förstärks när säkerhet mäts med enbart tekniska kriterier.

De samhällsekonomiska konsekvenserna är suboptimal resursallokering, systematisk underinvestering och ökade transaktionskostnader. Svensk informationssäkerhetsincidenter stämmer med denna tolkning, men artikelns huvudsakliga bidrag är teoretiskt: den visar hur en begreppsförskjutning kan förstärka redan kända marknadsimperfectioner. För att uppnå bättre samhällsekonomisk effektivitet krävs att informationssäkerhet återetableras som huvudbegrepp och att marknadsimperfectionerna adresseras med lämpliga styrmedel. Att integrera cybersäkerhetens specifika aspekter i ett bredare nationalekonomiskt ramverk som uttryckligen erkänner externalite-

ter, asymmetrisk information och incitamentsstrukturer är avgörande för välfärden i den digitala ekonomin.

REFERENSER

Akerlof, G A (1970), "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism", *Quarterly Journal of Economics*, vol 84, s 488–500.

Anderson, R och T Moore (2006), "The Economics of Information Security", *Science*, vol 314, s 610–613.

Arthur, W B (1989), "Competing Technologies, Increasing Returns, and Lock-in by Historical Events", *Economic Journal*, vol 99, s 116–131.

Carlsson, M (2024), "Chefen stoppade inte läcka – trots larm om försvarshemligheter", *Expressen*, 20 november 2024.

Dagens Nyheter (2024), "Kumla-hackarna kom åt 'i princip allting'", 7 november 2024.

ENISA (2024), "ENISA Threat Landscape 2024", European Union Agency for Cybersecurity, www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (hämtad 20 januari 2026).

European Commission (2020), "The EU's Cybersecurity Strategy for the Digital Decade", JOIN(2020) 18 final, eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52020JC0018.

European Union (2022), "Directive (EU) 2022/2555 (NIS 2)", *Official Journal of the European Union*, L 333, 27 december 2022.

European Union (2024), "Regulation (EU) 2024/2847 (Cyber Resilience Act)", *Official Journal of the European Union*, 20 november 2024.

Gordon, L A och M P Loeb (2002), "The Economics of Information Security Investment", *ACM Transactions on Information and System Security*, vol 5, s 438–457.

Gordon, L A, M P Loeb, W Lucyshyn och L Zhou (2015), "Externalities and the Magni-

tude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon–Loeb Model", *Journal of Information Security*, vol 6, s 24–30.

IBM Security (2024), "Cost of a Data Breach Report 2024", newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs.

ISO (2018), "ISO/IEC 27000:2018 Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary", International Organization for Standardization.

ISO (2022), "ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements", International Organization for Standardization.

ISO (2024), "ISO/IEC TS 27100:2024 Cybersecurity – Overview and Concepts", International Organization for Standardization.

Katz, M L och C Shapiro (1985), "Network Externalities, Competition, and Compatibility", *American Economic Review*, vol 75, s 424–440.

Kunreuther, H och G Heal (2003), "Interdependent Security", *Journal of Risk and Uncertainty*, vol 26, s 231–249.

MSB (2024a), "Till företag. Alla kan bidra till Sveriges cybersäkerhet. Du också", www.mcf.se/sv/publikationer/till-foretag-alla-kan-bidra-till-sveriges-cybersakerhet-du-ocks-a/ [nedladdad 2026-01-20].

MSB (2024b), "Resultatredovisning av Cybersäkerhetskollen 2024", Myndigheten för samhällsskydd och beredskap, <https://www.mcf.se/sv/publikationer/resultatredovisning-av-cybersakerhetskollen-2024--det-systematiska-cybersakerhetsarbetet-i-den-offentliga-forvaltningen> [nedladdad 2026-01-20].

Sjödén, K (2025), "Person med skyddad identitet röjd i läckan", *Svenska Dagbladet*, 17 september 2025.

SOU 2024:18, *Nya regler om cybersäkerhet*.