Framsyn som risikoradar

Hvordan kan scenarioanalyse forbedre cybersikkerhet?

ANATOLI BOURMISTROV er professor ved handelshøgskolen, Nord universitet og forskerkoordinator ved Nordområdesenteret. Han har mastergrad i romfartsteknologi Baltisk State Technical University, er siviløkonom fra Bodø, og har doktorgrad fra NHH. Hans forskningsinteresser ligger i fagområdene regnskap, økonomistyring, scenariometoder, økonomisk informasjon og mentale modeller.

SILJE AAKRE er nærings-ph.d.-kandidat i NC-Spectrum AS og tilknyttet handelshøgskolen ved Nord universitet. Hun forsker på cybersikkerhet i kraftbransjen.

SAMMENDRAG

Økt digitalisering og følgelig økt kompleksitet i samspillet mellom teknologi og mennesker skaper nye cybertrusler og øker sårbarhetsflaten for alle typer virksomheter. Tradisjonelle risikostyringssystemer er ikke lenger tilstrekkelig fordi de er reaktive, primært avdekker hendelser etter de har skjedd, og bygger på analyser av tidligere uønskede hendelser som sier lite om nye potensielle trusler. Utfordringen er hvordan en virksomhet kan tilegne seg ny kunnskap som gjør det mulig å forebygge hendelser før de inntreffer.

Denne artikkelen gir en konseptuell diskusjon av hvordan framsyn i form av scenarioanalyse kan forbedre cybersikkerheten og redusere organisatorisk sårbarhet. Vi analyserer litteratur innen fagområdene risikostyring, cyberrisiko og framsyn og diskuterer hvordan scenarioanalyser kan brukes av virksomheter for å løfte kunnskapen om potensielle trusler og øke beredskapen. Vi viser at framsyn kan motvirke en illusjon om kontroll som oppstår når tradisjonell, reaktiv risikostyring anvendes til å håndtere usikkerhet og såkalte sorte svaner. Scenarioanalyse utgjør en organisatorisk intervensjon som er ment å skape en arena for kunnskapsdeling mellom ulike aktører både innenfor og utenfor virksomheten. Scenarioer kan ses på som en risikoradar, blant annet gjennom å tilrettelegge for forebyggende og proaktive holdninger til metoder for risikostyring. Artikkelen konkluderer med at framsyn også kan bringe potensielle dilemmaer og fallgruver inn i virksomheter gjennom organisatorisk grensearbeid, selvoppfyllende profetier og trekk av en paranoid organisasjon.

INNLEDNING

Norske virksomheter møter i økende grad nye, innovative typer cybertrusler. Som motsvar benyttes både helhetlige risikostyringssystemer, internkontrollsystemer og overvåking av nettverkstrafikk i varierende omfang. Samtidig ser vi at mange virksomheter som benytter formelle systemer, fortsatt kan være sårbare. Dette er fordi styringsfunksjonen primært brukes til å avdekke hendelser etter at de har inntruffet, men ikke til å forebygge hendelser (Kulset & Meidelsen, 2020, s. 54). I likhet med dette baserer de fleste inntrengningsdeteksjonssystemene (IDS) seg på å varsle om

uønsket trafikk som allerede har blitt registrert i nettverket. Videre er hva som varsles om, typisk basert på historiske data om allerede kjente trusler.

En generell kritikk i litteraturen (Leitch, 2008, s. xiii) er at risikostyring i beste fall oppfattes som reaktiv og i verste fall bærer preg av sjekklister og pliktarbeid med liten effekt. Tradisjonell risikostyring basert på historiske data er ofte uegnet til å håndtere økende kompleksitet og usikkerhet med hensyn til potensielle trusler. God oversikt og kunnskap om cyberhendelser som har skjedd tidligere, garanterer ikke at virksomheter er godt forberedt på å håndtere andre typer cyberhendelser i framtiden. Risikostyringen bør bidra til bedret beredskap mot nye og ukjente typer cybertrusler. Ved å kun fokusere på avdekking er ikke virksomhetene proaktive i risikostyringen. Som følge kan risikoen for å bli rammet av nye, uønskede hendelser øke. På virksomhetsnivå kan en hendelse medføre blant annet tap av omdømme og økonomiske tap i form av bøter, skade på utstyr og tapt inntekt. På samfunnsnivå kan tilfeller hvor kritisk infrastruktur er rammet av cyberangrep, medføre fare for liv, helse og samfunnssikkerheten.

En mer proaktiv tilnærming til risikostyring er nødvendig for å møte trusler hvor menneskelige faktorer er involvert (Marshall, Ojiako, Wang, Lin, & Chipulu, 2019, s. 645). Nøkkelspørsmålet er: Hvordan kan virksomheter tilrettelegge for mer proaktiv og forebyggende risikostyring som også kan angi potensielle framtidige og foreløpig ukjente cybertrusler? Formålet med denne artikkelen er å diskutere konseptuelt hvordan framsyn kan brukes av virksomheter for å løfte kunnskapen om potensielle cybertrusler og bedre sin beredskap mot dem. Artikkelen bygger på analyse av litteratur om risikostyring, cybertrusler og framsyn med hovedvekt på scenarioanalyse. Drøftelsen illustrerer at scenarioanalyse kan være et nyttig verktøy for å sette virksomheten i stand til å lære mer om de ukjente cybertruslene. Dette kan stimulere til kontinuerlig organisatorisk læring for å bedre beredskapen mot potensielle cybertrusler.

Artikkelen tar først for seg kritikk av tradisjonell risikostyring. Deretter beskrives essensen i framsyn gjennom scenarioanalyse. Videre følger en diskusjon om hvordan scenarioanalyser kan møte kritikken av tradisjonell risikostyring. Avslutningsvis presenteres tre dilemmaer og fallgruver med scenarioanalyser, før konklusjon og behov for framtidig forskning.

KRITIKKEN AV TRADISJONELL RISIKOSTYRING

Risikostyring er i utgangspunktet ment for å hjelpe ledere med å håndtere usikkerhet. Det finnes mange normative rammeverk, fra for eksempel COSO og ISO, som framstiller tradisjonell risikostyring som en rasjonell prosess. I disse rammeverkene kan risikoen objektivt dokumenteres, måles, analyseres, rapporteres og revideres. Informasjon kan danne grunnlag for en virksomhets risikostyring. Tradisjonell risikostyring har til hensikt å avdekke uønskede hendelser og på den måten hindre at hendelsene inntreffer og truer virksomhetens måloppnåelse. Uønskede hendelser kan være alt fra datamanipulasjon og sabotasje til misligheter og svindel. Den tradisjonelle løsningen på problemene eller de uønskede hendelsene er å innføre rutinebasert risikostyring med sjekklister for å påse at regler og rutiner er på plass og fungerer (Moeller, 2011, s. 132). I de tilfellene hvor en uønsket hendelse likevel har inntruffet, kan man lære av egne feil og sette i verk bedre rutiner. Det er også slik at veldokumentert risikostyring er en legitimeringssak, fordi mange eksterne aktører, særlig myndighetene, ofte stiller krav til internkontroll og risikostyringssystemer. Av erfaring er det ofte slik at virksomheter kun tilfredsstiller minstekrav til slike systemer, og ikke gjør tiltak eller arbeid utover det de er pålagt. Utover dette har praktisering av tradisjonell risikostyring fått mye kritikk i risikostyringslitteraturen. Vi trekker her fram to: At tradisjonell risikostyring kan skape en illusjon om kontroll, og at den ikke er effektiv mot alle typer risiko, spesielt såkalte sorte svaner.

TRADISJONELL RISIKOSTYRING SKAPER EN ILLUSJON OM KONTROLL

Power (2009) argumenterer for at ambisjonen med risikostyring – å risikostyre alt – i virkeligheten kan gi motsatt effekt – risikostyring av ingenting. Mange ledere kan operere i tilstander vi betegner som en illusjon om kontroll. I dette ligger at mange har en tilbøyelighet til å overvurdere egen påvirkningsevne og kontroll. Her er troen på at man kan kontrollere risiko og påvirke framtidige positive resultater for sin virksomhet, større enn hva det objektivt sett er grunnlag for å anta (Schwenk, 1984, s. 121–122). Næringslivets sikkerhetsråd (2019, s. 12–13) fant en lignende tendens i sin undersøkelse av hybride trusler. Undersøkelsen

avdekket at 61 prosent av virksomhetene vurderer det som vanlig å bli utsatt for hybride angrep, til tross for at langt færre, 24 prosent, anså det som sannsynlig at deres egen virksomhet blir rammet. Illusjonen om kontroll over cybertrusler kan forsterkes av programvare, avtaler med anerkjente IT-miljøer og interne rutiner. Eksempelvis kan høy tiltro til leverandøren føre til at relevante spørsmål ikke blir stilt (Ceric & Holland, 2019, s. 183). Som resultat er evnen til objektiv vurdering av potensielle trusler og framtidige angrep sterkt redusert, og operative beslutninger tas på mangelfullt grunnlag.

I møte med cybertrusler kan menneskelige kognitive skjevheter medføre at tradisjonell risikostyring kommer til kort. Ulike kognitive skjevheter kan også virke sammen og ha en forsterkende effekt på hverandre. Bevisstgjøring rundt dette kan med andre ord påvirke risikostyringen. En utfordring er likevel at mennesker har begrenset kapasitet til å prosessere informasjon (Ceric & Holland, 2019, s. 183–184). Ikke-spesialister har i tillegg ofte problemer med å forstå de tekniske sidene ved cybertrusler, og det kan derfor bli krevende å ta gode beslutninger. Kognitiv skjevhetet medfører at beslutningstakere istedenfor å søke ny kunnskap, ekspertise og informasjon, heller strukturerer en problembeskrivelse og løsning basert på informasjon som støtter deres egne erfaringer, konklusjoner og fortolkninger (Ceric & Holland, 2019, s. 174).

Ifølge Soin og Collier (2013) bærer risikostyringen i enkelte virksomheter preg av sjekklister som ikke påvirker daglig drift, men skal demonstrere at interne rutiner er i samsvar med eksterne retningslinjer og krav. I slike tilfeller er risikostyringen først og fremst et legitimeringsverktøy – en illusjon om kontroll og en måte å oppnå legitimitet og gi ryggdekning på ved eventuelle hendelser. Det kan være sterke insentiver for å opprettholde en illusjon om kontroll både innad og utad. Graden av kontroll som investorer, myndigheter, kunder, konkurrenter og ansatte opplever, kan være avgjørende for forretningsmessige formål. I andre tilfeller kan manglende overvåkning og rapportering gi en illusjon av kontroll fordi eventuelle hendelser og trusler ikke kommer fram.

Paradoksalt nok kan det være vanskelig å sikre investeringer i cybersikkerhet fordi målet med tiltakene er at man *ikke* skal merke noe, eller at tiltakene *ikke* medfører noen merkbar konsekvens, det vil si fravær av hendelser. Det er heller motsatt: at avdelinger som utsettes for angrep, kan peke på manglende ressurser og oppnå økte budsjetter for å arbeide med sikkerhetstiltak etter at uhellet har vært ute.

TRADISJONELL RISIKOSTYRING ER LITE EFFEKTIV, SÆRLIG MOT SORTE SVANER

Risiko finnes i ulike former. Tradisjonell risikoanalyse, som beslutningstrær, forventet nytte og bayesiansk statistikk, er best egnet til å håndtere risiko i stabile omgivelser (Schoemaker, 1993, s. 208). De er med andre ord lite egnet til å håndtere høy usikkerhet og sorte svaner – de helt uventede hendelsene.Innen tradisjonell risikostyring forutsettes det ofte at uønskede hendelser kan dokumenteres, kvantifiseres og måles før det gjøres statistiske analyser av sannsynligheter og konsekvenser. På den måten vektlegger tradisjonell risikostyring hendelser som lar seg kvantifisere, dokumentere og kontrollere (Power, 2009, s. 851–852). I en verden som er blitt mer og mer kompleks som følge av blant annet ny teknologi, kan man godt lure på om omfanget av risikoer som faller under sorte svaner, øker betraktelig. Særlig gjelder dette cybertrusler. Manglende kunnskap om hendelser er et problem blant virksomhetene, også innen kritisk infrastruktur. I mange tilfeller kjenner ikke ofrene årsaken til at hendelsen inntraff (Norges vassdrags- og energidirektorat, 2017, s. 19–20). Det er også betydelig usikkerhet forbundet med når, hvor, hvordan og hvorfor de neste cyberhendelsene vil inntreffe, og hvem kan stå bak disse.

Det er viktig å merke seg at håndtering av kjente risikoer til en viss grad kan automatiseres. Dette gjelder også programvare som for eksempel kan blokkere e-post som lett lar seg identifisere som søppelpost eller svindelforsøk. Derimot må vellykkede angrep og arbeid med sorte svaner ses i sammenheng med det menneskelige aspektet. Tall fra Proofpoint (2019, s. 2) viser at under én prosent av angrepene via e-post som de observerte, benyttet systemsårbarheter. De resterende 99 prosentene utnyttet menneskelige faktorer som nysgjerrighet og tillit. Det er nettopp den menneskelige faktoren som gjør situasjonen uforutsigbar (Ceric & Holland, 2019, s. 184). Dette taler for en bredere forståelse av cybertrusler hvor enhver virksomhet kan betraktes som en del av et sosialt system med ulike menneskelige aktører. Når mennesker spiller en avgjørende rolle i vellykkede angrep, må også

mennesker være sentrale i å utforme systemer for å møte sorte svaner.

Oppsummert er det et behov for å bevege risikostyring fra etterlevelse av regler og sjekklister til gjennomtenkte ideer om potensielle framtidsscenarioer (Power, 2009, s. 852). Vi mener tradisjonell, reaktiv risikostyring er utilstrekkelig, især i situasjoner hvor kognitive skjevheter forsterker en illusjon om kontroll, og i møte med sorte svaner. Cybertrusler er ikke bare tekniske, men har også en menneskelig dimensjon. Håndtering av cybertrusler er dermed en sosial prosess hvor ensidig oppmerksomhet om teknologi kan hindre virksomheter i å oppfatte og forstå kritiske trusler (Parenty & Domet, 2019). I neste del skal vi se på hvordan framsyn og spesielt scenarioanalyse kan framstå som et viktig supplement, om ikke alternativ, til tradisjonell risikostyring.

FRAMSYN GJENNOM SCENARIOANALYSER: HVA OG HVORFOR?

Scenarioer kan ha ulike betydninger. For ingeniører eller sikkerhetseksperter indikerer begrepet i hvilken operasjonell kontekst ulike typer simuleringer, for eksempel beredskapsøvelser, finner sted (Schoemaker, 1993, s. 194–195). Når vi introduserer begrepet scenarioer i denne artikkelen, mener vi noe annet. Scenarioer er sammenhengende og troverdige beskrivelser om framtiden, og ikke operasjonelle kontekster, «projeksjoner, prediksjoner eller preferanser» (Cornelius, Van de Putte, & Romani, 2005, s. 93). Scenarioer er historier eller bilder av potensielle framtider som skapes gjennom anvendelse av framsyn som metode.

Scenarioanalyse er én av flere metoder for å arbeide med framsyn. I denne artikkelen brukes den intuitive logiske metoden, ofte kalt Shell-metoden, som beskrevet av Amer, Daim og Jetter (2013, s. 26–28). Arbeidet struktureres ved at diskusjonsgrupper identifiserer en rekke viktige faktorer, som økonomi, trender, politikk med flere, som kan forme framtidig utvikling. Metoden er således prisgitt gruppemedlemmenes kunnskap, evner og engasjement. Resultatet skal være troverdige beskrivelser av potensielle framtider. Slik blir beslutningstakere mer oppmerksomme på potensielle endringer i omgivelsene og hvordan disse kan møtes. Metoden er primært kvalitativ og egnet til å beskrive scenarioer som ikke lar seg modellere kvantitativt (Pollard & Hotho, 2006, s. 728). Det henvises til Amer og medforfattere (2013) for de som ønsker å fordype seg i ulike metoder.

UTFORDRE MENTALE MODELLER

Utover at scenarioer i seg selv er ment å være resultatet av framsyn, har scenarioer også andre formål. Som mennesker har vi en tendens til å tenke at framtiden kommer til å ligne nåtiden. Det er derimot ingen garanti for at framtiden, særlig i bransjer preget av høyt endringstempo, kommer til å ligne nåtiden. Scenarioer er et verktøy for å endre mentale modeller slik at virksomheten både kognitivt og kollektivt er bedre forberedt på å håndtere usikkerhet i omgivelsene. For å oppnå dette må scenarioene være sterke, troverdige og gjerne rikt beskrevet med detaljer (Schoemaker, 1993, s. 201–202). Dette åpner muligheten for å diskutere og korrigere antagelser og utarbeide forslag til reviderte strategier og innsatsplaner. Det er omdiskutert om scenarioanalyse faktisk klarer dette, og empiriske funn tilsier at scenarioanalyse har motsatt effekt, altså forsterkende effekt, på eksisterende antagelser og mentale modeller (Balarezo & Nielsen, 2017, s. 15–16).

TIDLIG VARSLING

Scenarioer er også ment å fungere som et system for tidlig varsling ved å stimulere til å identifisere potensielle trusler samt hvordan virksomheten kan respondere på ulike framtidige trusler og muligheter (Cornelius mfl., 2005, s. 95; Marshall mfl., 2019, s. 650). Dette betyr ikke at tidlig varsling gir noen garanti for effektiv risikostyring. Scenarioer skal ikke gi en følelse av kontroll over framtiden, men heller en bedre forståelse av mulige farer og en bevisstgjøring om at vår forståelse av samfunnet og handlinger er mangelfull (McDermott, 1996, s. 191, 194). Dette gjør at scenarioanalyse kan ha en viktig funksjon i å identifisere hendelser og utarbeide beredskapsplaner.

LÆRING

Scenarioer er ment for å skape læring. Økt bevissthet, forståelse og læring, som igjen skal gi bedre beslutninger og drift, skal være noen av resultatene av scenarioanalyse. På den måten framstår scenarioanalyse som et verktøy for å skape kontinuerlig læring i virksomheten. Dette gjelder på både virksomhetsnivå og individnivå (Balarezo & Nielsen, 2017, s. 9). Gjennom identifisering

og beskrivelse av (sjeldne) framtidige hendelser skal kognitiv treghet ved endringer reduseres.

Oppsummert er scenarioanalyse en prosess for organisatorisk intervensjon og læring om potensielle framtider som kan redusere svakhetene i tradisjonell risikostyring. I neste del ser vi på hvordan scenarioanalyse kan bistå med å bedre cybersikkerhet.

SCENARIOANALYSE SOM RISIKORADAR MOT CYBERTRUSLER

Det er mange grunner til at cybersikkerhet skal stå høyt på agendaen hos virksomhetsledere. I følge flere nasjonale og internasjonale retningslinjer skal cybersikkerhet inngå som en del av virksomhetsstyrenes overordnede ansvar for risikostyring og internkontroll. Dermed må man vurdere hvordan cybertrusler kan påvirke forretningsmessige aktiviteter i virksomheten. Siden cyberhendelser kan gi betydelige negative effekter for hele virksomheten, blir vurdering av cyberrisiko for viktig til at den kan overlates kun til IT-eksperter og eventuelt personell som arbeider direkte med cybersikkerhet. Parenty og Domet (2019) anbefaler at hver virksomhet skal utarbeide det de kaller cybertrusselhistorier. Historiene skal hjelpe virksomhetene med å oppdage trusler og prioritere og forberede mottiltak. Gruppa som skal utvikle historiene, skal bestå av ledere på ulike nivå, personell på operasjonsnivå, ansvarlige for IT-systemer samt andre relevante spesialister på de ulike områdene. Metoden adresserer systematisk koblinger mellom 1) kritiske forretningsmessige aktiviteter, 2) eksisterende IT-systemer, 3) cyberangrep og konsekvenser disse kan ha for virksomheten, og 4) gjerningspersoner, deres motivasjon og evner.

Metaforisk kan scenarioanalyse presenteres som en risikoradar. Radarmetaforen er hentet fra militær etterretning. Radaren kan ses på som et verktøy for proaktiv skanning av omgivelser for å oppdage og overvåke selv svake signaler om cybertrusler for å håndtere dem bedre. Radaren kan lokaliseres og posisjoneres i den nødvendige retningen. Med dette menes at scenariodiskusjoner kan rettes mot spesifikke temaer og analyseenheter. Ideen er at radaren kan forsterkes til å undersøke for eksempel en virksomhets sosiale trusselbilde. (Marshall mfl., 2019, s. 645, 650)

Siden cybertrusler har betydning for både strategisk og operasjonelt nivå, krever scenarioanalyse samhandling mellom ulike nivå i en virksomhet eller gruppe (Parenty & Domet, 2019). Overordnet nivå skal identifisere trusler som representerer en strategisk utfordring. Operasjonelt nivå skal identifisere trusler av operasjonell karakter og hvordan disse kan møtes. Dette krever samarbeid og kreativ tenkning i virksomheten og effektiv kunnskapsdeling mellom nivåene. En slik kunnskapsdeling kan foregå ved å etablere grupper som møtes regelmessig. Siden scenarioanalyse krever innspill fra individer, og noe arbeid dermed er individualisert, krever dette konstant utvikling av kompetanse hos ansatte, noe som i sin tur vil bidra til å forbedre kvaliteten på informasjon om usikkerheter og muliggjøre kreativ fortolkning av tilgjengelig informasjon.

Resultater av samhandlingsgrupper for scenarioanalyse kan være overordnede scenarioer som suppleres med en liste med operative innsatsplaner for ulike typer cyberangrep. Videre kan virksomheter teste slike innsatsplaner gjennom rollespill hvor hvert av scenarioene testes gjennom simuleringer og beredskapsøvelser. Dette kan bidra til bedre læring for eksempel gjennom koding av resultatene av rollespillet inn i reviderte innsatsplaner. (Marshall mfl., 2019, s. 655)

Det er kjent at scenarioanalyse blir brukt i norske virksomheter i ulike bransjer (Bourmistrov, Helle, & Kaarbøe, 2017). Vi har likevel begrenset kunnskap om hvordan scenarioer brukes, og kan brukes, til å bedre cybersikkerhet både i teori og praksis. Vi argumenterer for at framsyn og scenarioanalyse kan hjelpe virksomheter til å se styring av cybertrusler som en sosial prosess, og på den måten unngå en illusjon om kontroll.

FRAMSYN FOR CYBERSIKKERHET: POTENSIELLE DILEMMAER OG FALLGRUVER

Etter vår vurdering har bruken av framsyn og scenarioanalyse i virksomheter generelt positiv omtale i litteraturen. Det er likevel flere temaer hvor mer forskning er nødvendig for å klargjøre effekter av scenarioanalyse (Balarezo & Nielsen, 2017, s. 15–19; Amsteus, 2008, s. 63). Med tanke på dette ønsker vi å trekke fram tre potensielle dilemmaer og fallgruver for virksomheter. Vi anbefaler at også praktikere er oppmerksomme på disse, da de kan skape problemer for praksis. Dette gjelder organisatorisk grensearbeid, selvoppfyllende profetier og paranoide organisasjoner.

ORGANISATORISK GRENSEARBEID

Bruken av scenarioanalyse krever en diskusjon rundt hvem som skal være involvert i gruppa som skal produsere scenarioene. Som nevnt er gruppesammensetningen avgjørende for arbeidets resultat. En gruppe bestående av kun internt ansatte er det vanligste i den intuitive logiske metoden (Amer mfl., 2013, s. 28). Alternativt kan det åpnes for eksterne, for eksempel gjennom samarbeid med flere aktører i samme bransje. En tredje mulighet er å involvere flere interne eller eksterne interessenter, som myndigheter, kunder og leverandører. En fjerde mulighet er nettdugnad – hvor prosessen er åpen for alle. Det finnes ingen fasit her. Mens bred involvering av flere parter kan være gunstig for å få fram de viktigste perspektivene (Parenty & Domet, 2019; Schoemaker, 1993, s. 200), er dette også kostnads- og ressurskrevende for en virksomhet. Gieryn illustrerer at grensa for hva som skal tas inn i en profesjonell praksis eller ikke, er i endring. Med eksempler fra vitenskapen og akademia viser han at det også kan være insentiver for å holde seg til en engere krets, for eksempel for å unngå ansvar, bevare egen autonomi eller oppnå monopol på ressurser og profesjonell autoritet (Gieryn, 1983, s. 791–792). Litteraturen diskuterer også under hvilke omstendigheter samarbeid mellom virksomheter kan være hensiktsmessig (Wiener, Gattringer, & Strehl, 2018). Dette er særlig relevant for vurdering av cybertrusler. Det kan være behov for utvidet grensearbeid ved for eksempel å engasjere tidligere kriminelle og/eller opprette kommunikasjon med avanserte hackermiljøer (Marshall mfl., 2019, s. 645). Dette skaper uten tvil store etiske dilemmaer som må diskuteres og adresseres.

SELVOPPFYLLENDE PROFETIER

En selvoppfyllende profeti oppstår når forventningen til en hendelse skaper en atferd som øker sannsynligheten for at hendelsen inntreffer. Om vi ser på scenarioer som en teori om framtidige hendelsesforløp, kan det ifølge Ferraro, Pfeffer og Sutton (2005) være fare for at et bestemt scenario vinner tilhørere og etter hvert påvirker hvordan institusjonelt design og lederpraksis formes. Dette er fordi en institusjonalisert teori kan ha stor påvirkning på ideer, forutsetninger og bruken av profesjonelt språk. Det er absolutt en mulighet at virksomheter, særlig om de benytter seg av scenarioanalyse, avdekker en potensiell framtid som blir viet stor oppmerksomhet, og som gradvis muliggjør kollektiv handling, ikke bare internt, men også blant aktører utenfor virksomheten. Gjennom kollektive handlinger kan aktørene sammen påvirke til at nettopp en bestemt framtid materialiserer seg. Dette kan skje ved at et skadescenario lekker ut av virksomheten og gir hackermiljøer ideer til nye angrep.

PARANOIDE ORGANISASJONER

Overdreven konsentrasjon om ugunstige potensielle scenarioer kan gi tilsvarende sterk bekymring for at scenarioet skal inntreffe. Trusselbilder kan således generere vrangforestillinger om faktisk risiko, spesielt i tilfeller hvor relevant informasjon blir neglisjert (Schwarz, 2007, s. 20). Dette betegner vi som paranoide organisasjoner. Virksomheter kan spore av mot kontinuerlige søk etter andres skjulte hensikter og på den måten fremme mistillit og mistenksomhet. Når scenarioene skal diskuteres, kan slike virksomheter være så besatt av spesifikke framtider at de overproduserer negative bilder av nåtiden og framtiden, og overser alternative og for eksempel mer positive framtider, slik at disse ikke tas med videre i virksomhetens planer.

KONKLUSJON

Formålet med denne artikkelen var å diskutere hvordan framsyn kan brukes av virksomheter til å løfte kunnskapen om potensielle cybertrusler og øke sin beredskap. Gjennom analysen av litteraturen om både risikostyring og framsyn konkluderer vi med at bruken av scenarioanalyse som framsyn bør vurderes av virksomheter. Metoden trenger ikke erstatte tradisjonelle verktøy for risikostyring, men kan være et viktig supplement. Scenarioanalyse kan fungere som en risikoradar for å gi tidlig varsling om eventuelle hendelser og bidra til å redusere illusjonen om kontroll, siden potensielle trusler kan diskuteres i virksomheten på en systematisk måte av beslutningstakere og redusere kognitive skjevheter. Dette skjer gjennom å utfordre ledere og ansatte til å tenke proaktivt om cybertrusler og beredskap på både overordnet nivå, som hvordan cybersikkerhet passer inn i forretningsstrategien, og på operasjonelt nivå, som hvilken kombinasjon av innsatsplaner og tiltak som kan iverksettes gitt ulike scenarioer. Dette kan løfte kunnskapen om, og bedre beredskapen mot, potensielle cybertrusler. Vi advarer også om potensielle dilemmaer og fallgruver som er viktige å reflektere over ved scenarioanalyse, herunder

rollen risikostyring har i organisatorisk grensearbeid, selvoppfyllende profetier og paranoide organisasjoner.

Selv om det er gjennomført betydelig forskning på risikostyring, framsyn og cybersikkerhet hver for seg, har vi begrenset kunnskap om hvordan scenarioer som en del av risikostyring kan gi bedre cybersikkerhet. Vi etterlyser mer forskning som beskriver og analyserer beste praksis, for eksempel i virksomheter som allerede har tatt i bruk scenarioanalyse med positive eller negative resultater. Det kunne også vært interessant å benytte aksjonsforskning som metode på dette området, for eksempel ved at forskere i samarbeid med virksomhetene implementerer scenarioanalyse med formål om å bedre cybersikkerheten. M

REFERANSER

Amer, M., Daim, T.U., & Jetter, A. (2013). A review of scenario planning. *Futures*, *46*, 23–40. https://doi.org/10.1016/j.futures.2012.10.003

Amsteus, M. (2008). Managerial foresight: Concept and measurement. *Foresight*, *10*(1), 53–66. https://doi.org/10.1108/14636680810856026

Balarezo, J., & Nielsen, B.B. (2017). Scenario planning as organizational intervention: An integrative framework and future research directions. *Review of International Business and Strategy*, *27*(1), 2–52. https://doi.org/10.1108/RIBS-09-2016-0049

Bourmistrov, A., Helle, G., & Kaarbøe, K. (2017). Kreativ tenkning eller intelligent maskin? *Praktisk økonomi & finans*, *33*(1), 69–85. https://doi.org/10.18261/issn.1504-2871-2017-01-06

Ceric, A., & Holland, P. (2019). The role of cognitive biases in anticipating and responding to cyberattacks. *Information Technology and People*, *32*(1), 171–188. https://doi.org/10.1108/ITP-11-2017-0390

Cornelius, P., Van de Putte, A., & Romani, M. (2005). Three decades of scenario planning in Shell. *California Management Review*, *48*(1), 92–109.

Ferraro, F., Pfeffer, J., & Sutton, R.I. (2005). Economics language and assumptions: How theories can become self-fulfilling. *Academy of Management Review*, *30*(1), 8–24. Hentet 27.02.2020 fra http://jeffreypfeffer.com/wp-content/uploads/2011/10/AMR-Jan2005.pdf

Gieryn, T.F. (1983). Boundary-work and the demarcation of science from non-science: Strains and interests in professional ideologies of scientists. *American Sociological Review*, *48*(6), 781–795. Hentet 27.02.2020 fra https://www.jstor.org/stable/2095325

Kulset, E.M., & Meidelsen, K.H.R. (2020). Internkontroll som virkemiddel for å hindre underslag og svindel på innkjøpsområdet. *Magma*, *23*(1), 47–56.

Leitch, M. (2008). *Intelligent internal control and risk management: Designing high-performance risk control systems*. Aldershot: Gower.

Marshall, A., Ojiako, U., Wang, V., Lin, F., & Chipulu, M. (2019). Forecasting unknown-unknowns by boosting the risk radar within the risk intelligent organisation. *International Journal of Forecasting*, *35*(2), 644–658. https://doi.org/10.1016/j.ijforecast.2018.07.015

McDermott, W.B. (1996). Foresight is an illusion. *Long Range Planning*, *29*(2), 190–194. https://doi.org/10.1016/0024-6301(96)00007-6

Moeller, R.R. (2011). *COSO enterprise risk management: Establishing effective governance, risk, and compliance processes* (2. utgave). Hoboken: Wiley.

Næringslivets sikkerhetsråd. (2019). *Hybridundersøkelsen: Hybride trusler og hendelser mot norsk næringsliv*. Hentet 19.08.2019 fra https://www.nsr-org.no/getfile.php/1312167-1553166117/Dokumenter/NSR publikasjoner/Hybridundersøkelsen/Hybridundersøkelsen_web.pdf

Norges vassdrags- og energidirektorat. (2017). *Informasjonssikkerhetstilstanden i energiforsyningen*. Oslo. Hentet 21.06.2018 fra http://publikasjoner.nve.no/rapport/2017/rapport2017_90.pdf

Parenty, T.J., & Domet, J.J. (2019). Sizing up your cyberrisks. *Harvard Business Review*, *97*(6), 102–109. Hentet 27.02.2020 fra http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=139017616&lang=es&site=ehost-live

Pollard, D., & Hotho, S. (2006). Crises, scenarios and the strategic management process. *Management Decision*, *44*(6), 721–736. https://doi.org/10.1108/00251740610673297

Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society*, *34*(6–7), 849–855. https://doi.org/10.1016/j.aos.2009.06.001

Proofpoint. (2019). *Human factor report 2019*. Hentet 12.09.2019 fra https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf

Schoemaker, P. (1993). Multiple scenario development: Its conceptual and behavioral foundation. *Strategic management journal*, *14*(3), 193–213. https://doi.org/10.1002/smj.4250140304

Schwarz, J.O. (2007). Assessing future disorders in organizations: Implications for diagnosing and treating schizophrenic, depressive or paranoid organizations. *Foresight*, *9*, 15–26.

Schwenk, C.R. (1984). Cognitive simplification processes in strategic decision-making. *Strategic Management Journal*, *5*(2), 111–128.

Soin, K., & Collier, P. (2013). Risk and risk management in management accounting and control. *Management Accounting Research*, *24*(2), 82–87. https://doi.org/10.1016/j.mar.2013.04.003

Wiener, M., Gattringer, R., & Strehl, F. (2018). Participation in inter-organisational collaborative open foresight. A matter of culture. *Technology Analysis & Strategic Management*, *30*(6), 684–700. https://doi.org/10.1080/09537325.2017.1376045