Kurskod: SKDK11
Termin: Vårterminen 2024
Handledare: Rickard Andersson
Examinator: Cecilia Cassinger

”Operationen gick bra men patienten dog”

En kvalitativ hermeneutisk studie om intressenters uppfattning av cyberattacken mot Tietoevry

LISA GREEN & EMMI KRISCH SVÄRDBY

Lunds universitet
Institutionen för strategisk kommunikation
Examensarbete för kandidatexamen

Tack!

Vi vill framförallt rikta ett stort tack till vår handledare Rickard Andersson. Din hjälp har bidragit till nya insikter och utmanande vårt tänkande genom hela processen. Vi är särskilt tacksamma för din expertis som vi tagit del av och det tålamod du har visat oss.

Till sist vill vi tacka varandra för vår hängivenhet, vårt hårda arbete och vår vänskap. Det har varit ett varit ett nöje att arbeta tillsammans med detta projekt och vi ser fram emot framtida samarbeten.

Efter tre månader av hårt arbete avslutar vi nu det sista arbetet i vår kandidat. Vi intygar härmed att vi båda har bidragit likvärdigt till studien.

Lund, 19 Maj, 2024

Lisa Green

Emmi Krisch Svärdby

Abstract

As our society becomes increasingly digitised, a growing number of communication platforms emerge, necessitating interaction between individuals and organisations to sustain trust between them. One consequence of digitalisation that has gained more and more attention is the occurrence of cyber attacks, whose increased presence poses serious threats to individuals, organisations and society at large. The aim of our study is to investigate how stakeholders interpret and perceive the company Tietoevry's crisis communication after they suffered a cyberattack in 2024. By using hermeneutic principles and a thematic analysis, stakeholders' interpretations and reactions are decoded on the platform LinkedIn. The analysis is based on hermeneutic principles and the theories of Situational Crisis Communication Theory (SCCT) and Protection Motivation Theory (PMT). An abductive approach has been applied to enable a dynamic process in the analysis of empirical data and theory.

The results show that clear and transparent communication is essential to maintain trust between stakeholders and companies. Stakeholder reactions suggest a demand for timely and honest information and for the company to take responsibility and action to prevent future incidents. Our discussion highlights the importance of corporate behaviour and communication during crises, and how poor crisis communication affects the relationship with the organisation's stakeholders. The study contributes to a deeper understanding of the impact of crisis communication on trust and emphasises the importance of integrating stakeholder perspectives when designing communication strategies.

Keywords: Cyberattacks, crisis communication, stakeholders, stakeholder perspective, hermeneutics, SCCT, PMT

Number of characters including spaces: 99 997

Sammanfattning

I takt med att samhället digitaliseras ökar även tillgängligheten till olika kommunikationsforum där samspel mellan individer och organisationer är nödvändigt för att bibehålla förtroende mellan parterna. Som resultat av en stigande digital närvaro ökar även organisationers behov att hantera krissituationer i en kommunikativ kontext. En konsekvens av digitaliseringen som uppmärksammats mer och mer är förekomsten av cyberattacker, vars ökade närvaro utgör allvarliga hot mot både individer, organisationer och samhället i stort. Syftet med vår studie är att undersöka hur intressenter tolkar och uppfattar företaget Tietoevrys kriskommunikation efter att de drabbats av en cyberattack 2024. Genom att använda hermeneutiska principer och tematisk analys avkodas intressenters tolkningar och reaktioner på plattformen LinkedIn. Analysen baseras på hermeneutiska principer och teorierna situationsanpassad kriskommunikation (SCCT) och skyddsmotivationsteorin (PMT). Ett abduktivt tillvägagångssätt har tillämpats för att möjliggöra en dynamisk process i analysen av empiri och teori.

Resultaten visar att en tydlig och transparent kommunikation är väsentligt för att upprätthålla förtroendet mellan intressenter och företag. Intressenternas reaktioner indikerar en efterfrågan på snabb och ärlig information samt att företaget tar ansvar och vidtar åtgärder för att förebygga framtida incidenter. Vår diskussion belyser vikten av företags agerande och kommunikation under kriser, samt hur en undermålig kriskommunikation påverkar relationen med organisationens intressenter. Studien bidrar till en djupare förståelse av kriskommunikationens påverkan på förtroendet och understryker vikten av att integrera intressenternas perspektiv vid utformning av kommunikationsstrategier.

Nyckelord: Cyberattacker, kriskommunikation, intressenter, intressentperspektiv, hermeneutik, SCCT, PMT

Antal tecken inklusive blanksteg: 99 997

Innehållsförteckning

1. Inledning

I en era präglad av ständig utveckling och ett allt större beroende av digitala teknologier, står vårt samhälle inför nya utmaningar. Den snabba utvecklingen inom digitalisering har placerat Sverige i spetsen för flera områden inom digital utveckling och har resulterat i att landet rankas som Europas fjärde mest digitaliserade land (Europeiska kommissionen, 2023). Digitaliseringen är en stor drivkraft för innovation och tillväxt inom det svenska näringslivet, men kräver samtidigt robusta åtgärder för att säkra den digitala infrastrukturen (Svenskt Näringsliv, 2016). Trots Sveriges höga grad av digitalisering hänger säkerheten inte med där det idag finns anmärkningsvärda brister i Sveriges IT-säkerhetssystem, framförallt bland icke-statliga organisationer (Tidningen Näringslivet, 2023), och enligt National Cyber Security Index (NCSI) ligger Sverige på plats 16 i världen när det kommer till IT-säkerhet (2024).

Under 2023 utsattes Sverige för en kraftig ökning av antalet cyberattacker mot både statliga myndigheter och samhällsviktiga organisationer (MSB, 2024). En cyberattack är en medveten och målinriktad attack mot informationssystem, nätverk eller personliga datoranvändare, utförd via digitala medel, ofta med avsikten att stjäla, ändra eller förstöra information. Cyberattacker kan genomföras av antingen enskilda hackare, organiserade brottsliga grupper eller till och med stater, och de utgör ett allvarligt hot mot både individer och organisationer (Nationellt cybersäkerhetscenter, 2022). Enligt Myndigheten för samhällsskydd och beredskaps årsredovisning av it-incidentrapporter fördubblades antalet hackerattacker 2023 jämfört med föregående år (MSB, 2024). Det rapporterades totalt in 334 it-incidenter till MSB, varav 96 utgjordes av cyberattacker, vilket är en markant ökning jämfört med 2021 och 2022, då antalet rapporterade attacker var 48 respektive 40. Kring cyberattacker råder dessutom en stor tystnadskultur bland drabbade organisationer, där rädslan för skada företagets rykte ofta väger tyngre än behovet av öppenhet, vilket innebär att flera attacker inte rapporteras (IBM, 2023).

I detta klimat av osäkerhet och förändring understryker Carl-Oskar Bohlin, Sveriges minister för civilt försvar, vikten av att anpassa sig till ett *nytt normalläge* där cyberhot ses som en ständig närvaro snarare än en tillfällig avvikelse (SVT, 2024). Cyberattacker har blivit en integrerad del av många nationers krigföring, med Rysslands aggressiva användning av digitala medel som ett framträdande exempel (Cybersecrurity & Infrastructure Security

Agency, u.å). Ett exempel är det nordiska digitala tjänste- och programvaruföretaget Tietoevry som i början av 2024 utsattes för en cyberattack. Det var den ryska hackergruppen Akira som låg bakom attacken där flertalet av Tietoevrys datacenter lamslogs och påverkade en stor del av deras kunder, däribland flera svenska myndigheter (Tietoevry, 2024).

Denna nya verklighet kräver en omprövning av hur vi förstår och hanterar cyberattacker, inte minst ur ett kommunikativt perspektiv (SVT, 2024). Det ställer höga krav på organisationens kommunikativa förmåga att effektivt hantera kriser relaterade till cyberattacker gentemot sina intressenter. Indirekta kostnader, såsom skadat anseende och förlust av intressentförtroende, kan utgöra en betydande del av intrångets verkliga konsekvenser (PwC, 2020). Effekterna kan skapa en anseendekris för företaget, vilket i sin tur kan påverka företagets verksamhet på lång sikt (Kim et al., 2017). En effektiv kriskommunikation kan inte bara lindra den omedelbara krisen för en organisation, utan även spela en viktig roll i att återuppbygga och upprätthålla förtroende bland intressenter (Kim et al., 2017). Intressenternas reaktioner på en organisations kriskommunikation blir därmed avgörande för företagets förmåga att navigera i den digitala tidsåldern där det finns en digital osäkerhet.

1.1 Problemformulering

En stor del av den befintliga forskningen om cyberattacker idag och deras effekter på organisationer fokuserar primärt på de tekniska eller IT-relaterade aspekterna, med ett särskilt fokus på förebyggande åtgärder mot dessa hot (Yeom et al., 2021; Pourahmad & Hooshmand, 2023). Trots den betydande relevansen av denna forskning för att stärka organisationers säkerhet och försvar, är det viktigt att notera en brist i den befintliga forskningen när det gäller hur organisationer bör effektivt hantera sin externa kommunikation med intressenter under och efter att en attack har inträffat, samt se till intressenternas perspektiv och behov.

Inom området för strategisk kommunikation finns det omfattande forskning kring kriskommunikation, där teorin om situationsanpassad kriskommunikation (SCCT) en av de mest framstående och väl ansedda modellerna inom området (Coombs, 2007). Modellen utgör ett ramverk för de typer av respons som är tillgängliga för organisationer under en kris, däribland cyberattacker. Teorin har dock kritiserats av praktiker för att inte vara tillräckligt praktisk i tillämpningen (Avery et al., 2010). Det innebär att det är möjligt för praktiker att förstå det tillvägagångssätt de använder, men de tillhandahålls inte kriterier som gör det

möjligt för organisationer att avgöra vilken metod som ska användas. Det är också viktigt att komma ihåg att varje kris även involverar en mängd olika intressenter – från anställda och kunder till investerare och allmänheten (Coombs, 2023). Deras upplevelser, förväntningar och reaktioner kan vara avgörande för hur väl organisationen lyckas hantera och övervinna krisen. Trots detta tas inte deras perspektiv i beaktning i modellen, vilket betonar behovet av att vidare utforska och utveckla forskning inom området.

Denna kritik blir särskilt relevant i sammanhanget av dataintrång och cyberattacker. Traditionellt har sådana händelser betraktats som en del av offer-kluster, där organisationen ses som ett passivt offer utan ansvar för att ha orsakat händelsen (Coombs, 2007). Men i en värld där cyberattacker blir allt vanligare och mer sofistikerade måste vi ompröva denna synvinkel. Intressenterna, som ofta drabbas av konsekvenserna av attacker och som förlitar sig på organisationen för att skydda deras data och intressen, har också en viktig roll att spela i hur händelsen hanteras och kommuniceras.

Den större delen av studier kring kriskommunikation vid cyberattacker sker dessutom i en amerikansk kontext (Spanos and Angelis, 2016; Wang and Johnson, 2018; Wang and Park, 2017; Syed, 2019). Detta starka fokus på USA i tidigare forskning tyder på en betydande lucka i den svenska forskningen. Sverige och andra länder har sina unika kontexter och utmaningar när det gäller kommunikativa hanteringen av cyberattacker och dess konsekvenser för företag och samhälle som helhet. Företag som drabbats av cyberattacker har inte bara en direkt påverkan på sina egna verksamheter, utan kan även ha bredare effekter på samhället, inklusive förtroende för digitala system och samhällsviktiga funktioner (MSB, 2024). Därför är det nödvändigt att utforska och förstå den svenska kontexten när det gäller extern företagskommunikation efter dataintrång. Forskning inom cyberattacker och kriskommunikation av dessa slag är således inget outforskat ämne, däremot vill vi med studien belysa vad det innebär i en svensk kontext och i det nya samhälle vi befinner oss i, och framförallt lyfta intressenternas perspektiv.

1.2 Syfte och frågeställning

Syftet med studien är att bidra till forskningsfältet strategisk kommunikation genom att skapa kunskap om intressenters reaktioner och uppfattningar av extern kriskommunikation efter att en organisation drabbats av en cyberattack, specifikt inom den svenska kontexten. Detta

kommer vi att göra genom en analys av det svenska IT-företaget Tietoevry, som i januari 2024 drabbades av en omfattande cyberattack. Genom att tillämpa hermeneutiska principer, syftar studien till att avkoda de underliggande budskapen och meningarna i intressenters tolkningar och reaktioner. Studien använder en målmedveten datainsamlingsmetod för att selektivt samla relevant data från plattformen LinkedIn. För att uppnå vårt syfte kommer följande frågeställningar att härleda oss genom arbetet:

1. *Hur uppfattar intressenter Tietoevrys externa kriskommunikation efter cyberattacken?*

2. *Vilka underliggande budskap och teman framträder i intressenternas tolkningar?*

1.3 Avgränsning

Studiens frågeställning är relevant att studera i en bredare kontext, men på grund av begränsningar i tid och resurser fokuserar vår uppsats endast på den svenska kontexten genom vårt valda fall, Tietoevry. Studien tar avstamp i kriskommunikation inom forskningsfältet för strategisk kommunikation. Följaktligen kommer fallet och empirin studeras utifrån ett kommunikativt perspektiv, där IT-aspekter exkluderas. I analysen är studien avgränsad till intressenternas reaktioner och perspektiv på kriskommunikationen som följde cyberattacken och organisationens perspektiv granskas inte.

2. Forskningsöversikt

Forskningsöversikten ämnar att ge en omfattande sammanfattning av befintlig forskning kring intressenters tolkningar av kriser, med särskilt fokus på cyberattacker. Genom att utforska den befintliga litteraturen inom detta område, strävar översikten efter att identifiera kritiska gap i förståelsen av hur intressenter påverkas av och svarar på cyberattacker och deras kommunikation under krissituationer.

2.1 Kriskommunikation i samband med cyberattacker

Forskningen kring den externa kommunikationen efter en cyberattack tenderar att ha ett uppifrån-ned-perspektiv, där forskare använder förutbestämda teoretiska modeller som bästa praxis för att analysera hur företag hanterar kommunikationen vid cyberattacker. Dessa är oftast utformade utifrån ett organisatoriskt perspektiv, där fokus ligger på interna processer och strategier (Kulikova et al., 2012; Wang & Park, 2017; Wang & Johnson; 2018). Kim et al. (2017) är ett exempel på en studie som tillämpat en deduktiv metod för att undersöka hur dagstidningar tolkade kommunikationen vid dataintrång. Den deduktiva metoden kan dock begränsa tankegången och missa viktiga aspekter som inte passar in i den förutbestämda teorin, såsom intressenters perspektiv och behov. De framställda modellerna och ramverken kan dessutom ibland vara för snäva och begränsa möjligheterna att förstå den verkliga komplexiteten i hur företag kommunicerar med intressenter efter cyberkriser. Litteratur inom området tenderar alltså att ofta förbise intressenternas perspektiv.

I flera av dessa studier antas även SCCT-modellen som en förutbestämd ram, exempelvis i Wang och Park (2017) samt Wang och Johnson (2018). Studierna genomförs i dessa fall med en fast uppsättning kategorier, vilket riskerar att göra att det förbises andra förklaringar till resultaten. Det resulterar ofta i att de verkliga reaktionerna från intressenterna inte beaktas tillräckligt. Dessa studier verkar dessutom anta att intressenternas reaktioner kommer att följa mönstren enligt SCCT, som oftast appliceras för att förutsäga och förstå organisationers responsstrategier under kriser. Emellertid kan detta antagande begränsa vår förståelse för mångfalden av reaktioner och behov hos olika intressentgrupper som kan vara involverade i en krissituation. Att enbart fokusera på förväntade reaktioner enligt en teoretisk modell kan förbise viktiga nyanser och komplexiteter som kan påverka intressenters faktiska beteende. Det är känt att en dåligt hanterad relation mellan organisationer och intressenter kan vara en utlösande faktor för en kris (Coombs, 2023).

Vidare gör osäkerheten runt kriser det utmanande för organisationer att både förebygga och förutsäga när en kris kommer att uppstå (Wang & Park, 2017). Kriser uppfattas oftast större eller mindre än det de faktiskt är eftersom varje kris har både faktiska och uppfattade dimensioner av organisationens intressenter (Coombs, 2023). De faktiska dimensionerna handlar om själva händelsen och dess påverkan på organisationen, medan de upplevda dimensionerna handlar om hur olika intressenter (t.ex. anställda, kunder, allmänheten) tolkar och reagerar på krisen. Många kriser som organisationer står inför skulle inte utvecklas till kriser om det inte vore för intressenternas uppfattningar (Freeman, 1984). Intressenter har därmed en central roll och en stor påverkan i en organisation och deras perception på en händelse är avgörande huruvida situationen kommer att uppfattas som en kris (Freeman, 1984). Enligt Freemans intressentmodell är företag som tar hänsyn till intressenternas behov och intressen mer benägna att uppnå långsiktig framgång och överlevnad än de som enbart fokuserar på kortsiktiga vinstmål eller ägarnas intressen (Freeman, 1984; Coombs, 2023). Modellen bygger på idén att alla intressenter bidrar till och påverkas av företagets verksamhet, och därmed bör deras intressen beaktas i de strategiska beslutsprocesserna. Genom att erkänna och strategiskt engagera sig med dessa intressenter kan företag skapa värde inte bara för sina aktieägare utan för alla parter involverade. Detta synsätt förespråkar en mer inkluderande och etiskt ansvarsfull affärspraxis, som strävar efter en balans mellan ekonomisk framgång och samhällsansvar.

2.2 Intressenters ansvarstilldelning

Under en kris kommer intressenter att tillskriva ansvar och skuld till den drabbade organisationen, vilket kan variera beroende på krissituationer och strategier (Wang & Park, 2017). Hur intressenter uppfattar kriser spelar en betydande roll i att påverka krisutfallet och kan utgöra hot mot ryktet (Coombs, 2007). Organisatoriskt rykte kan sammanfattas som den samlade bedömningen eller uppfattningen av organisationens förmåga att leva upp till allmänhetens förväntningar när det gäller att säkra deras information (Syed, 2019). Denna definition betonar betydelsen av att ha en responsstrategi för att återställa kundernas förtroende för organisationens förmåga att hantera deras personuppgifter på ett ansvarsfullt sätt samt för att minska risken för ryktesförlust som kan uppstå till följd av en cyberattack (Office of the Information Commissioner, 2023).

För utforma en effektiv kommunikationsstrategi är det väsentligt att överväga de specifika omständigheterna i varje enskild kris, eftersom dessa direkt påverkar urvalet av de mest lämpliga svarsstategierna (Wang & Park, 2017). Attributionsteorin etablerar en länk mellan krisens natur och valda strategier, baserat på antagandet att individer bedömer orsakerna bakom händelser, särskilt de som är oväntade och negativa (Weiner, 1986). I en organisationskris kommer intressenter att göra attributioner kring orsaken till en kris och bedöma organisationens krisansvar. Coombs (1998) menar att om en organisation uppfattas kunna kontrollera en kris, kommer den att tilldelas mer ansvar för den krisen. Attributionsteorin tillhandahåller ett ramverk, inte bara för att identifiera de variabler som används för att bedöma hot mot ryktet i en krissituation, utan också för att integrera kriskommunikationsstrategier och krissituation i en teori om kriskommunikation. Coombs (1998) utvecklade senare teorin om situationsanpassad kriskommunikation för att analysera krissituation matchad till en rad av krissvarstrategier baserat på krisansvar och fann att skadan på organisationens rykte ökar i takt med att den uppfattade attributionen av krisansvar växer. I takt med att cyberattacker framträder som ett mer vanligt förekommande hot mot organisationer är det viktigt att undersöka hur intressenter skapar mening kring krisen och vilket ansvar de tillskriver organisationen.

2.3 Intressenters reaktioner på kriser i sociala medier

I dagens digitala samhälle är det enklare för intressenter att snabbt framkalla kriser om de upplever missnöje med en organisation. Fenomenet har förstärkts av samhällets ökade benägenhet att öppet uttrycka sina åsikter och farhågor gentemot organisationer genom internetplattformar (Coombs, 2023). När missnöjda intressenter lyckas kommunicera på ett sätt som resonerar med andra online och skapar en gemensam uppfattning eller opinion, kan det leda till att en kris uppstår. Denna interaktiva och dynamiska process av informationsutbyte mellan användare skapar en virtuell arena där organisationer måste navigera med stor försiktighet för att undvika att situationen eskalerar till en fullskalig kris. Legitim kritik som riktas mot organisationer av dess intressenter utgör dessutom ett direkt hot mot företagets rykte (Coombs, 2023). Denna dynamik förstärker vikten för organisationer att inte bara övervaka sociala medier noggrant, utan också aktivt engagera sig i dialogen för att effektivt hantera och lindra potentiella kriser.

Vidare kan användare på sociala medier skapa, ta emot och vidarebefordra sina egna negativa perspektiv på en krissituation, vilket ofta kringgår traditionella medier (Oh et al., 2013; Van der Meer & Verhoeven, 2013). Därför kan användare på sociala medier skapa och sprida sina personliga negativa perspektiv och åsikter kring en organisation efter en cyberattack. Användare på sociala medier kan också hamna i så kallade *ekokammare*, där de huvudsakligen konsumerar och interagerar med information som bekräftar deras egna åsikter och värderingar (Harris & Harrigan 2015). Denna tendens skapar en isolering från alternativa perspektiv och kan resultera i förstärkning av ensidiga åsikter och förvrängning av verklighetsuppfattningen. Denna dynamik kan i sin tur bidra till spridningen av negativa perspektiv och förvärra den allmänna uppfattningen om en organisation, särskilt om informationen sprids utan att vara föremål för kritisk reflektion eller granskning.

Inlägg i sociala medier som innehåller intensiv indignation, även kallat negativ word-of-mouth (nWOM), signalerar inte bara ett hot mot företagets anseende när det gäller dataintrånget, utan kan även ge upphov till ytterligare spridning av anseendehotande innehåll på sociala medier (Coombs, 2007; Pfeffer et al., 2014). Sådana hot kallas *rykteshot mot företag*, och kan definieras som en stor mängd inlägg på sociala medier som innehåller intensiv indignation, kritik eller klagomål mot ett företag som utsatts för en cyberattack (Pfeffer et al., 2014). Det lyfter fram behovet av att analysera intressenternas synpunkter och reaktioner. Försummandet av intressenternas perspektiv kan därför resultera i en förvärrad kris, som potentiellt hade kunnat undvikas med ökad förståelse för intressenternas behov och reaktioner.

Den snabba spridningen av information kan skapa en utmanande situation för organisationer, då en incident med dataintrång snabbt kan utvecklas till en fullskalig krissituation när den uppmärksammas av intressenter och media (Wang & Park, 2017). Det är också svårt för en organisation att dölja att de drabbats av en cyberattack. När det kommer till tidigare cyberincidenter upptäcktes 92% av intrången av en tredje part år 2011, vilket innebär att i de flesta fall kommer ett företag inte att kunna dölja vad som hänt och kommer att behöva etablera en dialog med externa intressenter (Kulikova et al., 2012). Dessutom kan upp till 28% av krisinformationen spridas globalt inom den första timmen (Syed, 2019). Det har även visat sig att en bristande respons inom 21 timmar kan lämna organisationen sårbar för kraftiga reaktioner och negativ publicitet på sociala medier, vilket ibland refereras till som en *rättegång på Twitter*. Därför måste organisationer vara förberedda på att ge en korrekt

förklaring av incidenten för att undvika offentlig kritik redan i början av krisfasen**.** Inom området finns det en bristande förståelse för intressenternas reaktioner som kan leda till missriktad kommunikation och därmed öka risken för negativa effekter av kriskommunikation. Genom att förbise intressenternas perspektiv löper man risken att skapa kommunikation som inte bara missar målet utan även kan resultera i att budskapet uppfattas felaktigt eller negativt av intressenterna (Syed, 2019).

2.4 Intressenters uppfattning och tolkning av en kris

Som nämnt spelar intressenterna en avgörande roll för att skydda företagsvärdet vid intrång Företagsrykte, som ingår i det bredare begreppet sociala utvärderingar, består av socialt konstruerade, kollektiva uppfattningar om företag (Kholekile et al., 2018; Coombs, 2023). Därför är det avgörande att upprätthålla en transparent och god kommunikation, särskilt i krissituationer (Wang & Park, 2017). En sådan kommunikation hjälper till att bygga förtroende och hantera företagets rykte på ett effektivt sätt.

God kommunikation kännetecknas av tydlighet, ömsesidig förståelse, respektfullt bemötande, aktivt lyssnande och anpassningsförmåga till olika situationer och kulturer (Cacciattolo, 2015). Det innebär också att kommunicera öppet och ärligt för att skapa förtroende hos intressenterna och undvika missförstånd och ryktesspridning. Dålig kommunikation, däremot, kännetecknas av bristande lyhördhet, otydlighet, brist på respekt och kan leda till missförstånd, frustration och konflikter (Cacciattolo, 2015). Att ha en dålig kommunikation i en kris kan bidra till allmän förvirring om situationen bland viktiga målgrupper, starta rykten och utlösa försäljning av företagets aktier (Kulikova et al., 2012). Samtidigt kan tydlig och bra kommunikation hjälpa till att snabbt engagera interna och externa intressenter i hanteringen av incidenter och hjälpa dem att fatta kloka beslut snabbare. Det kommer att öka den övergripande transparensen i en organisation, vilket är fördelaktigt för alla företag i tider av nya offentliggörande föreskrifter och ökad offentlig granskning.

2.5 Svenska intressenters uppfattning av digitaliseringen

Den identifierade bristen på forskning kring cyberattacker och kriskommunikation utanför USA har lämnat en lucka i förståelsen för fenomenet i länder som Sverige, där digitaliseringens framfart fortsätter att påverka både individer och samhället i stort. Rapporten *Svenskarna och Internet 2023* visar att en majoritet av svenskarna ser positivt på

digitaliseringens möjligheter, men också uttrycker oro för integritets- och säkerhetsrisker (Internetstiftelsen, 2023; Myndigheten för digital förvaltning, 2023). Denna dubbla hållning är ännu tydligare i ljuset av rapporten, som belyser att trots en hög digital anpassningsförmåga, så finns det en utbredd oro för datasäkerheten. En av de mest påtagliga orosapekterna rör cyberhot. 81% av svenskarna är oroliga för cyberattacker mot samhället (PwC, 2022). Dessa uppfattningar kan förklaras med bakgrund av den rådande ekonomiska osäkerheten med stigande inflation och en ökad misstro mot digitala organisationer, vilket påverkar hur teknologi och digitala lösningar mottas och förtros av allmänheten (Göteborgs-Posten, 2023). En central utmaning för den offentliga förvaltningen är att balansera öppenhet, för att främja insyn och deltagande, mot skydd av persondata för att garantera säkerheten. Denna balans är avgörande för att bygga tillit och förtroende hos användarna av digitala tjänster.

Enligt en rapport utfärdad av Radar 2021, som utvärderar kundförtroende och kännedom bland IT-leverantörer i Sverige framstod Tietoevry som en ledande aktör (Tietoevry, 2021). Denna studie, som involverade svar från över 640 organisationer inom både offentlig och privat sektor, visar att Tietoevry dominerar kategorin 'icke hjälpt kännedom', vilket indikerar en stark spontan närvaro i respondenternas medvetande. Företagets förmåga att skapa värde inom konsulttjänster rankas också högt, vilket stärker deras ställning som en pålitlig säkerhetspartner. Resultaten, som speglar ett starkt förtroende och erkännande inom branschen, understödjer Tietoevry strategiska riktning mot att vara förstahandsvalet för digital affärsförnyelse.

3. Teoretiskt ramverk

Det teoretiska ramverket ger en detaljerad beskrivning av de specifika teorier eller konceptuella ramverk, situationsanpassad kriskommunikation, hermeneutik och Protection motivation theory, som används för att vägleda denna studie. Kapitlet presenterar de centrala delarna och antagandena för dessa teorier, samt hur de är relaterade till studiens syfte och den forskningsfråga som testas.

3.1 Situationsanpassad kriskommunikation (SCCT)

En väletablerad teori för att formulera lämplig kriskommunikation är *situationsanpassad kriskommunikation* (SCCT), utvecklad av Timothy W. Coombs (2007). Modellen utvecklades som ett verktyg för att skapa förståelse för hur man skyddar ett rykte under en kris. SCCT kombinerar teori och empirisk forskning och förklarar kopplingen mellan krissituationer och hanteringsstrategier. Genom att ta hänsyn till faktorer före, under och efter en kris, identifierar SCCT olika krisscenarier och föreslår anpassade kommunikationsstrategier för varje situation (Coombs, 2007). Coombs utvecklade teorin för att fungera som ett flexibelt och tillämpbart ramverk i olika sammanhang och ger användare verktyg för att analysera och anpassa sin kriskommunikation baserat på de specifika omständigheterna. Den ska därför vara tillämpbar i alla typer av kriser (Coombs & Holladay, 2012). Genom att kartlägga situationsfaktorer ger SCCT en ram för att förstå och hantera kriser effektivt, samtidigt som den klargör organisationens ansvar i krissituationer (Sellnow & Seeger, 2021). I vår studie bidrar SCCT till en strukturerad ram för att analysera Tietoevrys kommunikationsstrategier, som sedan kommer att ligga till grund för analysen av dess effekt på intressenternas förtroende och stöd under krisen. Teorin är särskilt relevant för att bedöma kommunikationens effektivitet i att hantera intressenternas förväntningar och hur realistiskt företaget framställer situationen, vilket är centralt för att förstå eventuella perceptionsgap och kritik mot företagets kommunikativa hantering av attacken.

3.1.1 Krisfaktorer

De tre faktorer som tas i beaktning är *kristyp*, *krishistorik* och *tidigare rykte* (Coombs & Holladay, 2012; Sellnow & Seeger, 2021). Det är utifrån dessa praktiker kan skapa sig en uppfattning om bästa lämpade svarsstrategi.

Den första faktorn, *kristyp,* syftar till att beskriva den grundläggande naturen hos den kris som organisationen står inför. Detta innebär att man tittar på olika aspekter av krisen, inklusive omständigheterna kring dess uppkomst och vem som är ansvarig för den (Coombs, 2023). Om krisen uppträder som en olyckshändelse eller om organisationen är ett offer för yttre faktorer kan det ha en annan inverkan på den kriskommunikationsstrategi som krävs jämfört med om krisen är resultatet av avsiktliga handlingar från organisationens sida.

Den andra situationsfaktorn, *krishistoria*, refererar till organisationens tidigare erfarenheter av kriser. Om organisationen har en historia av framgångsrik krishantering eller har genomgått liknande kriser tidigare, kan det påverka hur intressenterna uppfattar och reagerar på den aktuella krisen. Å andra sidan, om organisationen har en historia av misslyckad krishantering eller tvivelaktiga handlingar i det förflutna, kan det skada förtroendet och öka svårigheten att hantera den nuvarande krisen. Denna faktor bidrar till att forma intressenternas kognitiva representation av den aktuella krisen och deras förväntningar på organisationens reaktion (Coombs, 2023).

Den tredje situationsfaktorn, *tidigare rykte*, handlar om hur andra såg på organisationen innan krisen inträffade. Det betyder att om organisationen hade ett gott rykte innan krisen, skulle det kunna påverka positivt hur intressenter ser på dem under krisen. Å andra sidan, kan ett tidigare dåligt organisationsrykte påverka negativt. Dessa krisfaktorer kan ge insikter i hur Tietoevrys intressenter reagerar på företagets kriskommunikation beroende på tidigare inställning.

3.1.2 Krishanteringsstrategier under en cyberattack

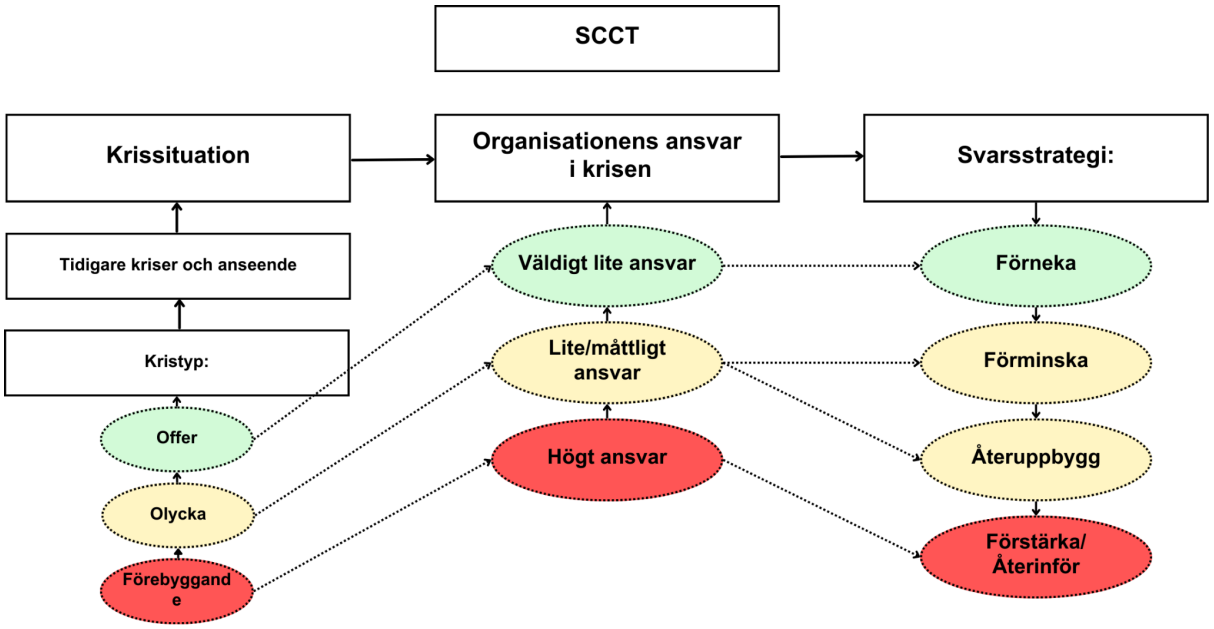
Enligt teorin klassificeras händelser ofta baserat på graden av kontroll som organisationen har över dem. Inom ramverket presenteras tre huvudkategorier av responsstrategier som organisationer kan tillämpa i samband med en kris: 1) Förnekelse, 2) Förminskning, och 3) Återuppbyggnad (Coombs, 2023).

Förnekelsestrategin används när det saknas bevis för en koppling mellan organisationen och den påstådda krisen, eller när organisationen kan demonstrera att ingen kris föreligger. Denna strategi kan innebära att man förnekar krisens existens eller pekar ut en extern part som

ansvarig. (1) Förminskningsstrategin syftar till att minska organisationens ansvar genom att betona brist på kontroll eller avsikt, eller genom att relativisera skadans allvar.

(2) Återuppbyggnadsstrategin innebär att organisationen tar fullt ansvar för krisen och erbjuder kompensation eller framför en ursäkt. Utöver dessa primära strategier lyfter SCCT fram (3) förstärkningsstrategin, som fokuserar på att framhäva organisationens tidigare positiva insatser och är särskilt effektiv när organisationen redan har ett starkt rykte och goda relationer med sina intressenter.

Inom ramen för SCCT faller en typisk cyberattack vanligtvis inom det så kallade offer-klustret (Heide & Simonsson, 2016). Denna kategorisering indikerar att den drabbade organisationen betraktas som en passiv mottagare av händelsen och har begränsad eller ingen kontroll över dess initierade faktorer. Att en händelse anses tillhöra offer-klustret innebär att organisationen ses som ett offer för yttre omständigheter, såsom attacker från cyberkriminella, och inte ansvarig för att ha initierat händelsen. Istället uppfattas organisationen som mottagare av konsekvenserna av attacken.



Modell 1: SCCT- modellen, egen utarbetning.

3.2 Hermeneutik inom kriskommunikation

I denna studie tillämpas hermeneutiken som en teoretisk ram för att analysera intressenters reaktioner och för att nå en fördjupad förståelse och tolkning av de komplexa innebörder som

framträder i samband med kriskommunikation. Som teori ger hermeneutiken en ram för att förstå hur kommunikation och mening skapas, överförs och tolkas inom olika sammanhang och kulturella kontexter (Prasad, 2018). Hermeneutiken betonar betydelsen av att tolka texter och erfarenheter i deras sammanhang och tar hänsyn till den subjektiva och kontextuella karaktären hos förståelseprocessen. Detta är av relevans för studien eftersom att kriskommunikation ofta innefattar mångfacetterade aspekter och tolkningar från olika intressenters perspektiv.

En central princip inom hermeneutiken är den komplexa naturen av tolkning, där texter och fenomen kan ge upphov till flera och ibland motsägande tolkningar (Prasad, 2018). Denna metodologiska ansats bygger på idén att mening och förståelse skapas i interaktionen mellan forskaren och det studerade objektet. Texten eller handlingen ses som en del av en större kulturell och historisk kontext. I sin moderna tillämpning inom samhällsvetenskaperna är hermeneutiken inte bara begränsad till texttolkning utan även till tolkning av sociala handlingar och interaktioner. Syftet med tillämpningen av hermeneutiken är att avkoda djupare lager av mening och kontextualisera dessa insikter inom de specifika omständigheterna som omger fenomenet (Prasad, 2018).

3.2.1 Hermeneutiska cirkeln

I kärnan av hermeneutiken finner vi den hermeneutiska cirkeln, en iterativ spiral av tolkning, där förståelsen om texten eller fenomenet förbättras genom att både analysera dess beståndsdelar och kontextualisera dem inom den övergripande helheten (Prasad, 2018). Denna metod är av grundläggande betydelse för att tolkningen av texter eller fenomen ska bli alltmer omfattande och nyanserad. Genom att belysa delarna i ljuset av den större helheten blir tolkningen mer komplett och djupgående. Denna ansats är särskilt värdefull i samhällsvetenskaplig forskning där målet är att förstå komplexa mänskliga beteenden och de subjektiva upplevelserna av de individer som studeras, som i vår studie (Prasad, 2018).

3.2.2 Misstankens hermeneutik och hermeneutik av tro

I den hermeneutiska traditionen finns det tre distinkta inriktningar, den existentiella, den allmänna tolkningsläran samt misstankens hermeneutik. Den sistnämnda, misstankens hermeneutik, använder forskaren kvantitativ data för att stödja tolkningen (Prasad, 2018). Misstankens hermeneutik betonar en kritisk och skeptisk inställning till texter eller fenomen.

Det syftar till att ifrågasätta och avslöja eventuella dolda motiv, underförstådda budskap eller maktstrukturer som kan finnas i tolkningen av texter eller handlingar. Tillämpningen av misstankens hermeneutik på texter eller fenomen blir det möjligt att identifiera och analysera eventuella bias, förvrängningar eller manipulationer som kan påverka tolkningen. Metoden uppmuntrar en djupare och mer kritisk analys av tolkningsprocessen för att nå en mer nyanserad förståelse av det studerade ämnet (Prasad, 2018).

Hermeneutik av tro är ytterligare en riktning som skiljer sig från den mer kritiska och skeptiska riktningen i misstankens hermeneutik. Hermeneutik av tro fokuserar på att förstå och tolka texter eller tal genom att inta en sympatisk och öppen inställning mot det material som studeras (Prasad, 2018). Inom forskning kan hermeneutik av tro tillämpas när forskaren eftersträvar ett djupt engagemang i de studerade texternas natur. Det används ofta i studier där författarens intentioner och kontextuella sanningar är av stor betydelse. Forskare kan använda denna metod för att försöka förstå en författares eller talares perspektiv på ett mer intuitivt och empatiskt sätt.

I studien kommer en växelverkan mellan hermeneutik av tro och misstankens hermeneutik, tjänar som en teoretisk grund för att tolka och förstå de underliggande betydelserna i kommunikationen och intressentreaktionerna. Denna ansats möjliggör en flexibel men djupgående analys, som kontinuerligt växlar mellan att försöka förstå intressenternas perspektiv genom en troende tolkning och samtidigt kritiskt granska dessa tolkningar genom misstankens hermeneutik.

3.3 Skyddsmotivationsteorin

En av de ledande teorierna som används för att förstå motivationen bakom individers säkerhetsbeteenden är skyddsmotivationsteorin (Protection motivation theory, PMT). Teorin utvecklades av Ronald W. Rogers för att förklara hur övertygande kommunikation påverkar beteendet, med tonvikt på kognitiva mekanismer som ligger bakom skälen till att följa eller inte följa ett rekommenderat beteende, samt hur rädsla kan påverka individers motivation och attityder (1975). PMT undersöker hur individer motiveras att agera skyddande i respons på uppfattade hot, vilket är särskilt relevant i kontexter där rädsla och hotuppfattning spelar kritiska roller i attitydförändringar och är därför lämplig att applicera i vår studie för att kunna uppnå syftet.

Rogers utvidgade sin ursprungliga teori för att inkludera hur individer förändrar sina attityder som respons på hotfull information. Denna utvidgade teoretiska ram betonar två huvudprocesser: *hotbedömning* och *hanteringsbedömning*. Dessa bedömningar samverkar för att forma individens motivationsstruktur att anta skyddsbeteenden (Rogers, 1983).

Hotbedömning är en kritisk psykologisk process där individen engagerar sig i en utvärdering av det upplevda hotet. Denna bedömning är inte bara begränsad till en ytlig förståelse av hotets existens utan omfattar en multifacetterad analys av flera kritiska dimensioner som formar individens reaktionsstrategier. Detta blir extra relevant i denna studie, då det kan förklara varför intressenter reagerar på ett visst sätt gentemot kriskommunikationen som följde efter cyberattacken mot Tietoevry. Hotbedömningsfaktorerna definieras som (1) i vilken utsträckning hotet anses vara allvarligt, (2) i vilken utsträckning individen anser att belöningen av att fortsätta med det riskfyllda beteendet överväger belöningen från att ändra sitt beteende och (3) individens sårbarhet inför hotet (Vance et al., 2012).

PMT har dessutom utvidgats till att omfatta informationskällor, intrapersonella egenskaper och tidigare erfarenheter i samband med hot och coping (Camerini et al., 2018; Rogers, 1983). Genom att integrera dessa komponenter tar den reviderade PMT ett mer holistiskt synsätt på förståelsen av beteendeintentioner. Denna tillvägagångssätt innefattar kontextuella faktorer såsom livsmiljö, informationskällor och sociala normer, vilka utgör ytterligare determinanter för säkerhetsbeteenden. Denna approach är särskilt relevant för vår studie då den tar hänsyn till aspekter hos individen som också är intressanta ur ett hermeneutiskt perspektiv och som kommer kunna förklara intressenternas reaktioner

Intrapersonella egenskaper omfattar bland annat sociala attityder och och upplevda sociala normer med avseende på hot och copingbedömning samt samt den beteendemässiga avsikten (Camerini et al., 2018). Slutligen kan tidigare erfarenheter av (cyber)sammanhanget sägas avgöra uppfattningar om risk och allvarlighetsgrad samt samt övertygelser om effektivitet i förhållande till ett specifikt beteende. I vår studie används denna utökade version av PMT för att ge oss insikter i hur intressenter uppfattar hotets allvar och sin egen sårbarhet, vilket är avgörande för att förstå deras reaktioner. Genom att bedöma hur intressenterna reflekterar över hotet hjälper PMT oss alltså att fånga deras riskmedvetenhet och därefter deras beteenden.

3.4 Tillämpning av teorierna i studien

För att uppnå vårt syfte att bättre förstå intressentreaktioner på Tietoevrys kriskommunikation efter cyberattacken kommer denna studie kombinera hermeneutiken med de presenterade teorierna, situationsanpassad kriskommunikation och skyddsmotivationsteorin. SCCT ger en stark strukturell grund som gör det möjligt att granska kommunikationsstrategierna och de responsmönster som framkommer från intressenterna. Denna analys fördjupas sedan genom integration av hermeneutiken och PMT, vilka båda bidrar till en ökad förståelse för de psykologiska och kontextuella faktorer som påverkar intressenternas reaktioner. PMT ger insikter i hur intressenterna uppfattar hot, medan hermeneutiken tillåter en dynamisk tolkning som navigerar mellan delen och helheten.

Vårt val att integrera Situationsanpassad kriskommunikation och Skyddsmotivationsteorin i vår kvalitativa studie om Tietoevrys kriskommunikation efter en cyberattack motiveras av deras potential att djupgående analysera och förstå intressentreaktioner. Trots att både SCCT och PMT ursprungligen utvecklades inom en kvantitativ forskningstradition kan de erbjuda värdefulla insikter i hur individer och grupper uppfattar och reagerar på kriser och risker. Denna studie fokuserar på att utforska hur, snarare än vad, vilket gör dessa teorier särskilt lämpliga då de tillhandahåller verktyg för att tolka och förstå dynamiken i kriskommunikation och dess effekter.

Inom ramen för vår abduktiva forskningsansats återvänder vi kontinuerligt till dessa teorier för att tolka våra empiriska data. Denna metod tillåter oss att iterativt förfina vår förståelse baserat på en kombination av teoretiska insikter och empiriska observationer. Detta angreppssätt är viktigt för att fylla det kunskapsgap som finns rörande kvalitativa aspekter av intressenters uppfattning av kriskommunikation i samband med cyberattacker.

4. Metod

Metodkapitlet nedan beskriver studiens metodik samt ett urval av empiriskt material. Vidare presenteras metodologiska överväganden som upptäcks under arbetets gång.

4.1 Vetenskapligt förhållningssätt

Människans uppfattning om verkligheten formar hur vi närmar oss kunskap och dess skapande (Björklund & Paulsson, 2014). Dessa förutbestämda uppfattningar influerar inte bara de metodval vi gör under forskningsprocessen, utan också hur vi tolkar och drar slutsatser från insamlad data. Därför är det av yttersta vikt att reflektera över och granska våra ontologiska och epistemologiska antaganden. Genom att göra detta kan vi få en djupare förståelse för hur våra grundläggande uppfattningar om kunskap och verkligheten påverkar våra forskningsval och resultat (Björklund & Paulsson, 2014).

I denna studie har det empiriska materialet samlats in och analyserats med en kvalitativ forskningsmetod, för att förstå intressenters reaktioner på Tietoevrys kriskommunikation. Kvalitativa metoder som fallstudier tillåter forskare att samla in detaljerade och djupgående data, vilket är avgörande för att kunna utforska och analysera materialet och diskursers olika dimensioner som är centrala för forskningsfrågorna (Silverman, 2022). Dessa metoder är dynamiska och kan skräddarsys för att möta de unika behoven i den specifika forskningskontexten. Tillvägagångssättet försöker förstå den mänskliga tolkningen och förståelsen av en socialt konstruerad situation. Tillvägagångssättet bygger på ord, vilket genererar en djupare beskrivning av studieämnet (Kvale & Brinkman, 2014). I motsats syftar den kvantitativa metoden till att testa teorin med numeriska data och förstår världen som något objektivt, vilket ytterligare motiverar valet av kvalitativ ansats som bäst lämpad för studien.

Studien ämnar att undersöka hur intressenter uppfattar den externa kriskommunikationen efter cyberattacken, därför har ett ontologiskt socialkonstruktivistiskt perspektiv antagits. Perspektivet utmanar föreställningen om en objektiv verklighet och belyser att verkligheten är socialt konstruerad (Silverman, 2022). Detta erbjuder möjligheten att analysera hur den sociala verkligheten konstrueras, rekonstrueras och bibehålls. Genom att tillämpa detta ontologiska ramverk kan forskningen utforska konstruktionen av verkligheten som omger intressenters uppfattning om cyberattacken mot Tietoevry, och belysa de dynamiska

processerna i hur denna typ av fenomen tolkas och uppfattas (Björklund & Paulsson, 2014). Inom vår studie har dessutom hermeneutiken tillämpats, som ser på sanning som något flytande och evigt föränderligt (Gadamer, 1997). Det är en syn som ligger väl i linje med principerna inom socialkonstruktivismen. Denna filosofiska inriktning har format vårt beslut att använda en kvalitativ metod där fördelen, enligt Flick (2018), ligger i dess förmåga att tolka och därmed avtäcka mångfasetterade tolkningar av komplexa fenomen såsom kriskommunikation.

I studien har ett abduktivt tillvägagångssätt använts, vilket har bidragit med flexibilitet till att integrera befintliga teorier med den empiriska datan som vi har samlat in (Flick, 2018). Detta tillvägagångssätt är särskilt värdefullt eftersom det gav möjlighet att dynamiskt jämföra och analysera det insamlade materialet mot befintliga teoretiska ramverk. Det möjliggör en utvärdering av om våra empiriska observationer stödjer existerande teorier eller om det krävs justeringar av vår teoretiska förståelse. Med tanke på att vårt forskningsämne är relativt outforskat och nytt, ger det abduktiva tillvägagångssättet en möjlighet att utforska fenomenet djupare och finna nya perspektiv och synsätt (Flick, 2018).

4.2 Datainsamling

Det råder ofta en otydlighet i kvalitativa studier angående hur deltagare valdes ut och hur forskarna valde ut sitt empiriska material (Bryman, 2008). I det följande avsnittet förtydligar och argumenterar vi för den valda insamlingsmetoden för att undvika detta. Vår ontologiska ansats kommer att ligga till grund för vårt tillvägagångssätt i såväl datainsamling som analysmetod. För att undersöka hur intressenter reagerar på kriskommunikation efter en cyberattack, kommer vi att basera vår studie på ett specifikt fall. Fallstudiemetoden gör det möjligt att samla in omfattande och detaljerad information om ett specifikt fenomen eller situation vilket således noggrant kan avgränsa vår undersökning till de aspekter vi finner mest relevanta utifrån vårt syfte (Schreier, 2012; Silverman, 2022).

Det empiriska materialet som har samlats in är officiella uttalanden och pressmeddelanden från Tietoevry, samt inlägg på LinkedIn från deras intressenter som svar på händelsen till följd av cyberattacken. Genom att integrera intressenternas egna åsikter och reaktioner i vår analys strävar vi efter att fånga en bredare bild av hur de upplever och tolkar organisationens hantering av krisen. Vid avgränsningen av det empiriska materialet granskade vi olika sociala

medieplattformar för att identifiera det mest relevanta materialet för vår analys. Valet föll på LinkedIn, eftersom vi observerade att diskussionerna där generellt håller en högre standard och ton, samt fann flest relevanta åsikter kring fallet jämfört med andra sociala medier. Andra källor har alltså exkluderats från studien på grund av att vi ansåg att de var bristande i lämplighet och/eller tillförlitlighet när det kom till att tillhandahålla relevant material för vår analys. För att välja inlägg och kommentarer som var mest lämpliga användes sökord som *Tietoevry cyberattack LinkedIn, Tietoevry cyberattack LinkedIn 2024*. Inlägg som inte hade några kommentarer eller inte pratade om cyberattacken exkluderades.

Vi har använt en målinriktad urval-strategi, mer specifikt kriteriebaserat urval, för att välja inlägg och kommentarer som liknar varandra, ligger nära i tiden och återspeglar ämnet (Schreier, 2012). 6 textinlägg och 71 kommentarer samlades in, där 20 intressenter och deras kommentarer sedan valdes ut då de ansågs representativa för reaktionerna. Empirin samlades in från händelsens start, 19 januari 2024 till 19 april 2024. Vi ansåg att ett medvetet urval var mest lämpligt i vår studie då det låter oss jämföra prover som är homogena för att urskilja trender och mönster (Schreier, 2012). Vissa av citaten och orden som använts i analysen har översatts från engelska till svenska, vilket kan påverka språkets innebörd något.

4.3 Val av fall

Valet av fall till vår studie är motiverat av flera faktorer. För det första har cyberattacken mot Tietoevry haft en betydande inverkan på en stor del av befolkningen, på varierande nivåer, eftersom Tietoevry hanterar flera stora organisationers IT-säkerhet. Bara genom Statens servicecenter uppskattas 60 000 personer vara direkt drabbade (Lindh & Sundström, 2024). Förutom det hade Filmstaden problem med att sälja biobiljetter under en hel vecka och flera e-handelsbutiker, som Stadium och Rusta, låg nere under en längre period. Som ett resultat av attacken har även 20 års data från Tandvårds- och läkemedelsförmånsverket, den myndighet som beslutar om vilka läkemedel som ska ingå i högkostnadsskyddet, gått förlorade (Dagens Nyheter, 2024). Det stora antalet drabbade individer och samhällspåverkan genom detta gör det särskilt viktigt och intressant att analysera intressenters reaktioner på attacken. Genom att analysera dessa reaktioner kan vi identifiera vilka kommunikativa behov och förväntningar de har från Tietoevry.

Vidare är det av betydelse att notera att denna cyberattack inte endast har drabbat de traditionellt erkända samhällsviktiga institutionerna. Den har även påverkat en rad andra organisationer som möjligen inte betraktas som lika centrala för samhällets funktion, men trots detta påverkar en stor del av svenska befolkningen. Denna aspekt är av särskild relevans då den belyser behovet av att inte enbart fokusera på att skydda de mest uppenbara målen för cyberattacker utan även på att skydda organisationer som kan ha en indirekt eller mindre framträdande inverkan på samhället. Dessutom, som poängterats i inledningen, är dessa typer organisationer ofta mindre skyddade från cyberattacker (TN, 2023). Trots att vissa effekter kan framstå som triviala vid första anblicken är det viktigt att notera att dessa har en kaskadeffekt som påverkar samhällets dynamik på olika sätt. Detta gör fallet både relevant och ändamålsenligt för att förstå den aktuella dynamiken och utmaningarna i dagens samhälle när det kommer till krishantering och kommunikation vid cyberattacker och hur denna sedan tas emot av befolkningen.

4.4 Analysmetod

Den analysmetod som har tillämpats i denna studie för att analysera det empiriska materialet är en kvalitativ hermeneutisk metod. I denna metod intar språket en central roll, och det är avgörande att forskarna är medvetna om språkets betydelse i sina tolkningar (Prasad, 2018). Genom att kritiskt analysera sina tolkningar under arbetets gång kan forskarna skapa ny förståelse. Hermeneutiken hävdar att fördomar hos tolkaren inte behöver betraktas som något negativt. Gadamer introducerade begreppet produktiva fördomar, som tvärtom kan de vara till nytta och bidra till en fördjupad förståelse av den studerade texten (Prasad, 2018). Genom att integrera tidigare erfarenheter och förståelse i tolkningsprocessen skapas en mer nyanserad tolkning av empirin.

Hermeneutisk tolkning används främst för att studera enskilda fall, vanligtvis genom fallstudier. Inom traditionen följer forskaren inte en strikt, steg-för-steg metod för att tolka texter. Istället baseras tolkningen på generella principer som vägleder forskarens analys (Kvale & Brinkmann, 2009). Den hermeneutiska tolkningen kan med fördel kombineras med andra tolkningsprocesser för att hjälpa till att strukturera och tolka materialet (Langemar, 2008). Tematisk analys som är en utforskande innehållsdriven metod, baseras på att forskaren läser och sorterar det empiriska materialet för att kunna identifiera mönster, teman och underliggande diskurser som formar analysen (Guest et al., 2012). Den undersöker mönster

och korrelationer i intressenters uppfattningar av Tietoevrys kommunikation. Genom att analysera antalet utsagor kan forskaren skapa tabeller som illustrerar återkommande ord eller mönster. Den hermeneutiska metoden kan således effektivt kombineras med en tematisk analys, där kodningsprocessen i den tematiska analysen ger en strukturerad och djupgående förståelse av vårt fallstudieobjekt.

En tematisk analys kräver en bredare tolkning och engagemang från forskare, eftersom de måste förstå både vad som sägs och vad det kan innebära för dataanalysen. Det var därför ett abduktivt tillvägagångssätt tillämpades, vilket innebär en dynamisk växelverkan mellan teori och empiriska data (Flick, 2018). I detta sammanhang fungerade vårt teoretiska ramverk, särskilt hermeneutiken, som analytiska glasögon för att identifiera och anpassa kategorier (Schreier, 2022). Metoden bidrog till en systematisk strukturering av det insamlade materialet, där olika segment tilldelades förutbestämda kategorier i en kodningsram för att fokusera analysen och identifiera relevanta teman som speglar reaktioner från intressenter på Tietoevrys responsstrategier inom kriskommunikation. Teman har justerats efter behov under analysprocessen, vilket är i linje med den hermeneutiska cirkelns iterativa och flexibla natur (Schreier, 2022). Det möjliggör en dynamisk interaktion mellan oss som forskare, teori och empiriska data.

4.4.1 Teman och kodningsschema

Genom att granska empirin har teman identifierats och valts ut. Dessa teman presenteras i tabell 1. Genom att identifiera teman i en analys kan läsaren bättre förstå de huvudsakliga idéer och begrepp som diskuteras i texten (Flick, 2018). Det kan också hjälpa till att organisera och strukturera analysen, så att den blir tydligare och mer sammanhängande. Dessutom kan identifiering av teman hjälpa till att avslöja underliggande budskap och toner i LinkedIn-inlägg, vilket ger en djupare förståelse av dess innehåll och perspektiv (Flick, 2018). Teman kan berätta något om hur intressenterna reagerar på Tietoevrys externa kriskommunikation och kommer därför att utgöra ett stöd till analyskapitlet. De olika teman identifierades genom en djupgående uppdelning och granskning av det använda språket. Till exempel, genom att identifiera underliggande diskurser och attityder, placerades de olika texterna in i 5 övergripande teman som vi tycker speglar den övergripande tonen.

Teman	Kod
Kriskommunikation	Vaghet och otydlighet i Tietoevrys kriskommunikation
	Kritik mot företagets kommunikativa hantering av attacken
Realism vs. framställning	Perceptionsgap: Finns det en märkbar skillnad mellan företagets framställning och intressenternas uppfattning av situationens realitet
	Förskönande av allvarliga incidenter
Ansvarstilldelning	Företaget bär huvudansvar för incidenten
	Företaget bär lite eller inget attribuerat till ansvar
Uppfattad allvarlighet och sårbarhet	Hög riskmedvetenhet: Intressenter känner en stark oro för potentiella eller faktiska risker som kommuniceras
	Låg riskmedvetenhet: Intressenter känner en minimal oro för potentiella eller faktiska risker som kommuniceras
Intressentanalys och förståelse	Inblick i intressenternas behov och förväntningar
	Intressenters känslomässiga respons på företagets berättelse

Tabell 1: Framarbetade teman och tillhörande koder, egen utarbetning.

4.5 Metodreflektion

Studien använder material som är lätt att spåra och tillgängligt för allmänheten, vilket ökar forskningens trovärdighet och uppriktighet (Tracy, 2010). Som i de flesta metoder och analyser finns det för- och nackdelar med vår valda analysmetod. I denna studie har ett socialkonstruktivistiskt perspektiv använts för att analysera kriskommunikation. Detta tillvägagångssätt främjar en genomgående granskning av de antaganden och attityder som påverkar tolkningen och i detta fall, av kriskommunikation (Björklund & Paulsson, 2014). Studiens tillvägagångssätt, är baserat på hermeneutik, som betonar tolkningens roll och tillåter en djupgående förståelse av hur intressenter tolkar och reagerar på kriskommunikationen från Tietoevry efter en cyberattack. En vanlig kritik mot den socialkonstruktivistiska ansatsen och hermeneutiska analysmetoden, är att de kan vara subjektiva och svåra att generalisera ifrån, eftersom tolkningar kan variera beroende på forskarens perspektiv och förutfattade meningar (Prasad, 2018). Det kan vara utmanande att bedöma exaktheten eller tillförlitligheten i tolkningarna eftersom olika forskare kan komma till olika slutsatser baserat på samma data. Samtidigt anser vi att subjektiviteten i vår studie kan betraktas som en styrka, då den kan ge större förståelse för det undersökta fenomenet och de individer som studeras (Prasad, 2018).

Vidare har en tematisk analys använts och kritiken, där den främsta kritiken är att metoden tenderar att vara mindre subjektiv än hermeneutiken, men kan vara normativ ur ett vetenskapligt perspektiv (Boreus & Bergström, 2018). Forskarens tolkning och förståelse har ett inflytande på analysen av den insamlade empirin (Guest et al., 2012). Det påverkar studiens kvalitet, speciellt om studien innefattar fler än en forskare. För att hantera denna fråga, och för att stärka studiens kvalitet, dokumenterades all insamlad, kodad och analyserad data tydligt för att underlätta resonansen och öka uppriktighet av forskningsprocessen. Detta tillvägagångssätt underlättade även för en konsistent och jämförbar förståelse av det insamlade materialet. Den hermeneutiska inriktning ställs ofta i motsättning till en tematisk analys, eftersom den prioriterar djupgående tolkning framför bredare kvantifiering genom kodningsscheman och systematisk analys av data (Prasad, 2018). Vi ansåg dock att en tematisk analys kunde komplettera den hermeneutiska analysen i vår studie. Tematiseringen underlättade tolkningen av den empiriska datan och bidrog till en mer strukturerad uppdelning av materialet. Eftersom studien tillämpar en abduktiv ansats är kodningsschemat en flexibel process och anpassas kontinuerligt under forskningsprocessen i enhet med en hermeneutiska cirkeln, vilket skiljer sig från den strikta kodningsprocess som vanligtvis förknippas med enbart tematisk analys.

Vid diskussion om etiska dilemman är det viktigt att ta itu med vissa etiska restriktioner (Hallin & Helin, 2018). Samtliga intressenter vars kommentarer som samlats in kommer att vara anonyma i vår studie, med syfte att skydda deras identiteter. Alla intressenter tilldelas ett nummer utifrån ordningen deras kommentar eller inlägg presenteras i analysen, mellan 1-20 (Hallin & Helin, 2018).

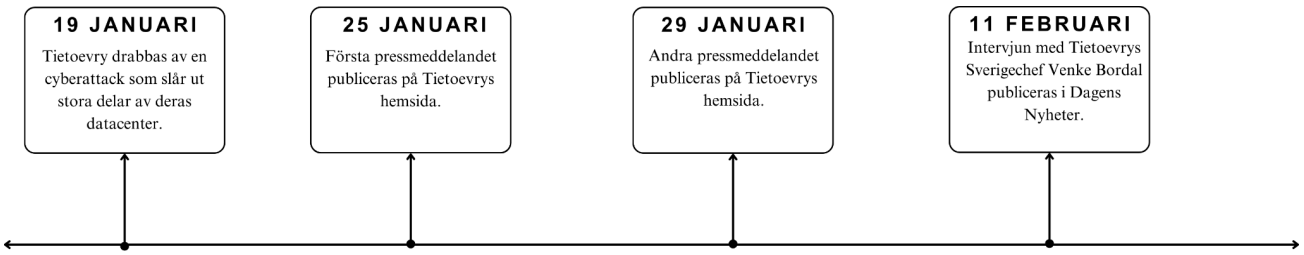
5. Analys

I följande avsnitt bryts det empiriska materialet ner och granskas med hjälp av teman som återfunnits i empirin. Analysen grundas i en hermeneutisk tematisk analys och har utgångspunkt i hermeneutiska principer, situationsanpassad kriskommunikation och skyddsmotivationsteorin. Analysen har delats upp i olika delar för att skapa en tydlig struktur och underlätta läsbarheten. Första delen utgörs av en kort redogörelse för fallet med en efterföljande analys av de identifierade kriskommunikationsstrategierna. Andra del av analysen består av en detaljerad beskrivning av intressenternas reaktioner på LinkedIn på kommunikationen från Tietoevry efter cyberattacken.

5.1 Vinjett

Natten mellan den 19 och 20 januari 2024 drabbades den skandinaviska IT-jätten Tietoevry av en omfattande cyberattack som slog ut stora delar av deras centrala datacenter (Tietoevry, 2024). Eftersom företaget är en IT-leverantör för ett stort antal svenska organisationer blev som tidigare nämndes, konsekvenserna stora för det svenska samhället. Som svar på attacken genomförde företaget flera kommunikativa åtgärder för att informera sina kunder och allmänheten om situationen. Inledningsvis publicerades ett flertal pressmeddelanden där företaget bekräftade attacken och underströk dess allvar och vikten av att hantera dess följder. I dessa meddelanden framhöll Tietoevry de åtgärder som hade gjorts för att säkra sina system och begränsa skadan, inklusive samarbeten med ledande cybersäkerhetsexperter och lagförande myndigheter. Trots Tietoevrys strävan att upprätthålla transparens och öppenhet, underminerades deras ansträngningar snabbt av en utbredd skepticism och spekulativa tolkningar.

Den 11 februari 2024 publicerades en intervju i Dagens Nyheter med Sverigechefen för Tietoevry, Venke Bordal, som blev särskilt uppmärksammad (Dagens Nyheter, 2024). I uttalandet kommunicerade Bordal att *det inte fanns några brister i Tietoevrys säkerhetssystem* (DN, 2024). Uttalandet väckte många reaktioner och möttes av kritik, både bland sakkunniga och intresserade medborgare. En diskussion blossade upp om Tietoevrys ansvar för att säkra viktiga system och huruvida företagets bedömning av sina säkerhetsåtgärder var adekvat. Händelsen skapade en ytterligare dimension av granskning och utvärdering av företagets förmåga att hantera och kommunicera om sina it-säkerhetsfrågor.



Modell 2: Tidslinje över händelsen och inledande kommunikativa insatser från Tietoevry, egen utarbetning.

Teorin om situationsanpassad kriskommunikation ger ett ramverk för att förstå hur organisationen bör hantera sin kommunikation under en kris. I fallet med Tietoevrys hantering av deras cyberattack ger Bordals uttalanden en insikt i hur företaget använder kriskommunikationsstrategier utifrån SCCT-modellen för att hantera krisens effekter på deras rykte. I den uppmärksammade intervjun förklarade Bordal att det *inte är något som har brustit i Tietoevrys it-säkerhet* (DN, 2024). Detta uttalande kan tolkas som en del av en förnekelsestrategi. Enligt SCCT används förnekelse när organisationen antyder att ingen kris föreligger eller att krisen är resultatet av externa aktörers handlingar (Coombs, 2007). Denna svarsstrategi ska enligt modellen vara lämplig, då en cyberattack ska falla inom offer-klustret, där organisationen har lite ansvar för krisen och den är ett resultat av externa faktorer bortom dess makt. Trots att Bordal erkänner att de inte vet hur angriparna tog sig in, syftar hennes kommentar till att avvisa föreställningar om interna fel eller brister, vilket potentiellt minskar företagets upplevda egna ansvar.

Förminskningsstrategin är återigen tydlig när Bordal sedan antyder att cyberattacker är en bredare samhällsutmaning och inte bara ett problem isolerat till TietoEvry. Genom att säga att *Det kanske händer vilken dag som helst på vilket annat företag som helst* (DN, 2024). I citatet använder Bordal en teknik som normaliserar händelsen för att minska dess upplevda allvarlighet (Coombs, 2007). Strategin syftar till att minimera skadans allvar genom att framhäva att sådana händelser är vanliga, men svåra att helt förhindra. Trots användningen av förnekelse och förminskning, inkluderar Bordals strategi inte tydliga inslag av återuppbyggnad, såsom att erbjuda ursäkter eller kompensation. Detta kan tyda på en avvägning mellan att försöka minska omedelbar skada på företagets rykte och att undvika att ta på sig mer ansvar än nödvändigt, vilket kan vara väsentligt i väntan på ytterligare utredning och information om händelsen.

5.2 Vaghet och otydlighet i Tietoevrys kriskommunikation

Ett centralt tema som framträtt i genomgången av empirin är *kriskommunikation*. Intressenterna delade sina uppfattningar och åsikter om uttalandet från Bordal och diskuterade företagets hantering av händelsen, särskilt deras kriskommunikation. I flera kommentarer framträder en tydlig känsla av frustration och upprördhet över Bordals uttalande och företagets generella hantering av krisen. Bland samtliga 77 observationer som gjordes i empirin fanns det ingen som värderade Tietoevrys kriskommunikation positivt.

Intressenterna verkar påtagligt upprörda och irriterade över hur VDn kunnat påstå att det inte funnits brister i säkerhetssystemet. *Såhär kan det inte få fortsätta. Det är ju direkt okunnigt att säga att man inte har några säkerhetshål* (Intressent 1, 2024, LinkedIn). Kommentaren vittnar om en oro över företagets förståelse för situationens allvar och dess förmåga att kommunicera effektivt med sina intressenter. Det går också att urskilja en tydlig uppfattning om att företaget antingen inte tar situationen på allvar eller inte är transparent i sin kommunikation kring sina säkerhetsprotokoll. Användningen av ordet *okunnigt* kan antyda att intressenten uppfattar företagets påståenden som inte bara felaktigt, utan även som ett tecken på bristande kompetens eller medvetenhet hos företaget. En mer ingående tolkning av reaktionen kan indikera att intressentens oro inte enbart berör faktiska säkerhetsåtgärder, utan även speglar en bredare skepsis om företagets ethos och trovärdighet.

Men det är en katastrofal kriskommunikation att säga att de inte har några brister (Intressent 2, 2024, LinkedIn). I kommentaren går det att tolka det som att intressenten anser att Tietoevry förnekar eller bagatelliserar händelsen, vilket tyder på en uppfattning om att företaget inte tar situationen på tillräckligt allvar eller är villigt att erkänna bristerna i sin hantering av krisen. Intressentens användning av ordet *katastrofal* visar ett djupt missnöje och besvikelse över företagets agerande. Ordvalet kan tolkas som en stark emotionell reaktion som inte bara kritiserar de specifika kommunikationshandlingarna utan även kastar tvivel över företagets generella förmåga att hantera kriser. Det framgår tydligt att intressenterna upplever att företagets kommunikation lider av flera av de karaktärsdrag som tidigare forskning har associerat med bristfällig kommunikation i kris, som bristande transparens, oklarhet i budskapen och en upplevd brist på respekt för intressenternas oro och åsikter (Cacciattolo, 2015). Att intressenterna har starka reaktioner på kommunikationen skulle därför kunna förklaras av den tidigare forskning som påtalat vikten av att ha en god och

transparent kommunikation under en kris (Kulikova et al., 2012). Bristerna som har påtalats i Tietoevrys sätt att kommunicera kan ha förvärrat situationen och ökat risken för negativa reaktioner och förtroendekriser.

Samtidigt uttrycker flera intressenter en önskan om att företaget skulle ha intagit en mer öppen och reflekterande kommunikationsstrategi för att återställa förtroendet och föra dialogen framåt. Det förekommer flera förslag om att erkänna bristerna i säkerhetssystemet och lova att lära av händelsen, vilket pekar på vikten av att visa sårbarhet och ödmjukhet i krishanteringen för att återupprätta förtroendet hos intressenterna. Precis som Syed (2019) poängterat riskerna med, verkar det finnas en bristande förståelse för intressenternas perspektiv som i detta fall verkar ha lett till en ökning av de negativa effekterna av kriskommunikationen. Tietoevry beskriver situationen på ett sätt som inte matchar med intressenternas förväntningar på kommunikationen. En intressent uttrycker sitt missnöje på följande sätt:

> *När makthavare börjar uttala sig tvärsäkert om sin egen skuldlöshet trots mängder av motbevis uppstår ett Orwellianskt språkbruk som får oss att ifrågasätta sanningen som väsen. Som får oss att tvivla på vår egen förmåga att förstå, då absurditeten är så uppenbar. Som konstform är denna nutidssurrealism otvivelaktigt kittlande, men som vägvisare för en mer rättvis värld direkt bedräglig* (Intressent 3, 2024, LinkedIn).

Det framkommer en kritisk syn från intressenten på hur makthavare använder sitt språk för att förvränga sanningen och manipulera uppfattningen om händelser. Intressenten menar att när makthavare, Bordal i detta fallet, kan ses förneka sin egen skuld trots tydliga motbevis, skapas en Orwelliansk dynamik där sanningen förvrängs och allmänheten börjar tvivla på sin förmåga att förstå verkligheten. Det orwellska språkbruket syftar på liknande användning av språk i verkligheten, där politiska eller auktoritära organisationer använder ord och fraser för att vilseleda, desinformera eller kontrollera befolkningen (Orwell, 2017). Det kan inkludera uttryck som alternativa fakta för att förneka uppenbara sanningar. Det används för att skapa en slags verklighetsförvrängning där sanningen blir subjektiv och regeringens agenda dikterar det språkliga landskapet. Genom en kritisk tolkning kan detta indikera på att intressenten upplever att företaget försöker missvisa eller vilseleda sina intressenter och att de använder

ett propaganda-liknande språk via makt. Fler intressenter verkar dessutom dela denna uppfattning:

> *Jag tolkade det också som ett försök på den typen av taktik av verklighetförnekande som politiker numer kommer undan med, att bara hävde en helt alternativ verklighet och sedan stenhårt hålla sig till den och inte låtsas om att den är helt påhittad. Frågan är hur man som IT-chef tror att man ska ha samma savant liknande magi som Trump har. Den här tekniken är nog svårare än man tror* (Intressent 4, 2024, LinkedIn).

Även här framhäver citatet en kritisk syn på hur kriskommunikation hanteras i samband med cyberattacken. Intressenten pekar på en parallell till politiska kommunikationsstrategier som kännetecknas av att skapa och upprätthålla en alternativ verklighet. Denna strategi av verklighetsförnekelse, som citatet antyder, jämförs med den tidigare amerikanske presidenten Donald Trumps förmåga att navigera i offentliga narrativ, trots uppenbara motsägelser med faktiska händelser. Intressenternas kritik kan tolkas både som en kritik direkt mot företagets val av kommunikationsstrategi, men även som en större samhällskritik där denna typ av språkbruk blir allt vanligare.

Reaktioner från intressenterna indikerar en tydlig uppfattning om att Tietoevry använder bortförklaringar och undviker att ta ansvar för situationen; *Nånannanismen vår tids största pandemi. Det är nån annans fel/skuld/ansvar mm. Aldrig mitt* (Intressent 5, 2024, LinkedIn). Denna uppfattning är särskilt relevant när vi betraktar kommunikationen utifrån Coombs SCCT-modell, och det så kallade "offer-klustret" som en organisation enligt modellen ska hamna inom vid en cyberattack (Coombs, 2007). Enligt SCCT bör denna typ av kriskommunikation vara lämplig, eftersom Tietoevry också är ett offer i situationen och enligt modellen är det den bästa svarsstrategin för att förminska krisen och/eller skylla ifrån sig. Kommentaren från intressent 5 exemplifierar och visar på en vanligt förekommande reaktion där det är uppenbart att intressenterna inte köper Tietoevrys argument och aktivt motsätter sig företagets kriskommunikation. Detta pekar på en potentiell brist i effektiviteten hos denna typ av svarsstrategi. Det kan bero på flera faktorer, som att fenomenet cyberattacker inte längre är så ovanligt, vilket kan göra att intressenterna är mer misstänksamma och kräver tydligare ansvarsutkrävande från företaget. Dessutom skulle det kunna bero på att intressenterna som

vi undersökt har en viss kunskap om IT-säkerhet och cyberattacker, vilket gör dem mer benägna att ifrågasätta företagets oskuld och kräva ett mer proaktivt ansvarstagande.

Det bör också uppmärksammas att en betydande andel av kritiken riktas direkt mot VDn, vilket signalerar en tydlig missnöjdhet med hennes roll och ansvar i hanteringen av krisen. Denna fokuserade kritik mot Bordal kan tolkas som ett uttryck för intressenternas behov av att identifiera ansvariga och söka efter förklaringar för företagets agerande, där Bordal blir en typ av syndabock. Genom att peka ut VDn som ansvarig för kommunikationen och strategin under krisen ger intressenterna uttryck för en önskan att se ledarskap och transparens från högsta nivån i organisationen. Det är samtidigt viktigt att notera att denna riktade kritik också kan spegla en bredare oro över företagets kultur och värderingar, där VDns uttalanden och agerande kan ses som en representation av företagets övergripande hållning gentemot kunder, anställda och samhället i stort. I detta avseende kan kritiken mot VDns kriskommunikation uppfattas som vagt och otydligt och tolkas som en signal om ett behov av förändring och förbättring på en djupare nivå inom organisationen.

5.3 Tietoevrys försköning av cyberattacken

Inom temat "realism vs. framställning" framträdde två centrala koder: *Perceptionsgap* och *förskönande av allvarliga incidenter*. Genom koderna har det gått att identifiera en tydlig dissonans mellan företagets kommunicerade bild av händelsen och intressenternas uppfattningar. Dessa fynd belyser en distinkt dissonans mellan hur Tietoevry presenterar situationen och hur intressenterna uppfattar verkligheten. Kholekile et al. (2018) menar att intressenterna har en stor påverkan på företagsvärdet vid ett intrång och kan påverka utfallet hur företaget porträtteras efter en kris. Utifrån det är det viktigt att företaget och intressenterna delar uppfattningen av händelsen för att undvika missförstånd och konflikter som kan förvärra krisen.

Perceptionsgapet manifesterar sig tydligt mellan Tietoevrys kriskommunikation och intressenternas uppfattning när företaget försöker framställa en bild av pålitlig IT-säkerhet, där Bordal säger: *Vi vet inte hur man har attackerat här. Men ja, jag vågar påstå att vi har en väldigt hög säkerhet* (DN, 2024). Denna framställning verkar inte stämma överens med intressenternas uppfattning, som upprepade gånger påpekar att det måste funnits en brist i säkerheten, som framgår i följande kommentar:

> *[...]De vet bara att de själva garanterat inte har brustit i något led. Men angriparna har väl knappast tillämpat magi [...] nog måste det funnits säkerhetshål? Det vet vi inte, menar Sverigechefen Venke, för Tietoevrys säkerhet är absolut tillräckligt hög* (Intressent 3, 2024, LinkedIn).

Citatet från intressent 3 speglar ett tydligt gap mellan företagets uppfattning och den bild som intressenterna har. Intressenten ifrågasätter företagets självsäkra ton, vilket antyder att Tietoevry framställer sin säkerhetsnivå som högre än vad som verkar rimligt utifrån intressentens synvinkel. Den ironiska undertonen i kommentaren förstärker denna skeptiska inställning och antyder en brist på förtroende för företagets påståenden. Genom att använda ironi uttrycker intressenten tvivel kring företagets påstående om en *absolut tillräckligt hög* säkerhetsnivå och antyder att det är osannolikt att angriparna inte skulle kunna hitta några sårbarheter.

Som nämnts under temat kriskommunikation framhåller Cacciattolo (2015) att en realistisk, ansvarsfull och öppen kommunikation ofta leder till bättre utfall i termer av rykteshantering och kundförtroende. Det är tydligt att den generella uppfattningen inte är att Tietoevrys kommunikation är varken realistisk eller ansvarsfull, snarare tvärtom. I kommentarsfältet kan kommentarer som *"Vi har inte brustit i vår säkerhet" men ändå hackades ni i en av de största hackning attackerna i Sverige* och *affärsmässig mörkläggning* (Intressent 6, 2024, LinkedIn; intressent 7, 2024, LinkedIn) reflektera en bredd inom missnöjet och misstron från intressenterna. Kommentaren ifrågasätter inte bara företagets påståenden om säkerhet utan också dess förmåga att ärligt erkänna och adressera sina svagheter. Dessa uttalanden kan tolkas som indikationer på att det finns en dissonans kring företagets uppfattning om IT-säkerheten och intressenternas.

Som Coombs (2023) och Freeman (1984) har påpekat, är det inte bara de faktiska dimensionerna av en kris – såsom händelser och dess direkta påverkan – som formar en krisupplevelse, utan också hur dessa händelser uppfattas och tolkas av intressenterna. Felhantering av dessa uppfattningar kan eskalera en hanterbar situation till en fullskalig förtroendekris. Det är därför kritiskt att Tietoevry utvecklar en kommunikationsstrategi som inte bara adresserar de faktiska riskerna utan också bygger och underhåller förtroende genom transparent och ärlig dialog med sina intressenter. Detta understryker betydelsen av att

hantera intressentrelationer och kommunikation noggrant för att förhindra en 'kris i krisen' där intressenternas missnöje och misstro kan förvärra situationen ytterligare. Detta verkar delvis vara fallet för Tietoevry, där det går att tolka det som att det uppstått en kommunikativ kris som en konsekvens av den valda kriskommuniaktionsstrategin.

Inom teman *realism vs. framställning* skapades även koden *förskönande av allvarliga incidenter,* där det identifierades att intressenterna upplever att företaget försöker mildra perceptionen av krisens allvar. Ett exempel på detta är kommentaren:

> *Hennes uttalande är ungefär lika motsägelsefullt som det gamla läkar-skämtet: "Operationen gick bra men patienten dog."* (Intressent 8, 2024, LinkedIn).

Citatet antyder att företaget försöker att nedtona händelsens allvar, och intressentens reaktion speglar en misstro och nästan cynisk syn på kommunikationen. Coombs (2023) menar att det under kriser skapas en virtuell arena där företaget måste vara försiktig i sin kommunikation för att situationen inte ska eskalera. Det verkar vara fallet här, där Bordals intervju kan ha misslyckats med att lugna situationen och istället förstärkt intressenternas oro och skepticism. Den snabba kommunikationen på sociala medier leder till en bred spridning, vilket understryker vikten av att kommunikationen är välformulerad och genomtänkt redan från början. Om kriskommunikationen är bristande, som intressenten antyder i citatet, kan det lämna organisationen sårbar med negativ publicitet på sociala medier. I en annan kommentar lyfter intressenten fram Tietoevrys stora konsekvenser efter cyberattacken, där den säger:

> *Kaskadeffekterna av attacken är stora och har spridit sig till företagets kunder och kunders kunder. I dagsläget är 120 myndigheter, ett antal kommuner och regioner samt ett antal privata företag drabbats* (Intressent 9, 2024, LinkedIn).

Citatet står i kontrast till Tietoevrys initiala kommunikation, som menade att det inte funnits några brister i säkerheten. Denna diskrepans framkallar en negativ word-of-mouth-effekt, där intressenternas upplevda realitet av situationen avviker markant från företagets initiala uttalanden. Diskrepansen mellan företagets framställning och den uppfattade situationen kan leda till förlorat förtroende, speciellt om intressenterna känner att deras risker och eventuella

förluster inte har tagits på allvar (Kulikova et al., 2012). Det går att urskilja en uppfattning om att företaget inte tar situationen på tillräckligt allvar eller är villigt att erkänna bristerna i sin hantering av krisen, vilket verkar provocera intressenterna starkt.

Samtidigt går det att argumentera för att de övervägande negativa kommentarerna är en effekt av så kallade ekokammare, och att intressenternas reaktioner påverkas och provoceras av varandra. Denna samverkan skapar en förstärkt negativ bild av företaget, vilket inte endast isoleras till individuella kommentarer utan blir en del av en bredare offentlig diskurs. Denna mekanism förstärker och upprätthåller den negativa bilden, vilket potentiellt kan skada företagets långsiktiga relationer med sina intressenter och minska dess förmåga att effektivt återhämta sig från krisen. Det understryker vikten av att företag inte bara adresserar de initiala negativa kommentarerna, utan också engagerar sig i en genuin och öppen dialog för att bryta denna negativa feedbackloop och återuppbygga förtroendet hos sin intressentbas.

5.4 Intressenters tillskrivning av ansvar

Det råder delvis delade meningar om vem som är ansvarig för cyberattacken som Tietoevry drabbades av. Bland de observationer som gjorts i den empiriska datan under tema tre, *ansvarstilldelning*, kan vi konstatera att det finns både de som menar att Tietoevry bär huvudansvar för incidenten. Samtidigt har vi identifierat ett flertal kommentarer som menar att Tietoevry har antingen lite eller inget ansvar för händelsen. De flesta intressenterna antar dock en tydlig och nästan ironisk attityd gentemot Tietoevry, särskilt när det gäller företagets förnekande av primärt ansvar för krisen. Denna skeptiska syn kommer till uttryck i kommentarer som utmanar företagets ansvarsfriskrivning på ett nästan sarkastiskt sätt kan ses i följande exempel:

> *Är fortfarande chockad över hur man kan beskylla kunder för problem i miljöer man själv säljer och implementerar* (Intressent 10, 2024, LinkedIn).

Genom den underliggande tonen i kommentaren kan intressentens ställning tolkas som provocerad och frustrerad. Det verkar som att hen är upprörd över att företaget försöker skifta ansvaret för problemen till kunderna, trots att det är företaget självt som säljer och implementerar miljöerna där problemen uppstår. Detta antyder på en uppfattning om att företaget undviker att ta ansvar för de problem som uppstår i de miljöer de erbjuder. Personen

kan känna att företaget borde ta ett större ansvar för att säkerställa att deras produkter och tjänster fungerar korrekt och inte lägga skulden på kunderna. Den provocerade tonen kan också indikera en känsla av maktlöshet inför företagets agerande och ansvarsfrågan i denna situation. När citatet tolkas utifrån misstankens hermeneutik framträder en insikt om de maktstrukturer som möjliggör denna ansvarsförskjutning. Det kan ge oss en förståelse för hur företaget potentiellt kan manipulera den offentliga bilden för att skydda sitt rykte. Det kan signalera en ojämn maktbalans där företaget har möjlighet att forma narrativet till sin fördel (Westlund, 2015). Detta pekar på att intressenterna uppfattar att ansvarsfördelningen är orättvis och att företaget bör ta större ansvar för att lösa eventuella problem.

Det är ju bevisligen så att de åtgärder som fanns på plats inte räckte, att påstå något annat är direkt självmål (Intressent 11, 2024, LinkedIn). I citatet framgår det återigen att intressenten betraktar det som ett misstag att försöka undvika ansvar i situationen. Även här går det att dra paralleller till SCCT-modellen och det förväntade utfallet av kriskommunikationen. Kommunikationen från Tietoevry verkar få motsatt effekt från vad man enligt modellen kan förvänta sig, utifrån att organisationen befinner sig i offer-klustret (Coombs, 2018). En förklaring till att många intressenter tilldelar organisationen den höga nivån av ansvar kan förklaras av fakta pekat på att det råder en ökad misstro mot digitala organisationer bland svenska invånare (PwC, 2020). På grund av den redan skeptiska inställningen kan det bli svårare för Tietoevry att upprätthålla förtroendet från intressenterna under krisen.

Samtidigt finns det också intressenter som verkar tycka att det rör sig om ett större, mer systematiskt problem i vårt samhälle, där vi inte har en tillräcklig digital mognad för att kunna hantera denna typ av kriser. I intervjun med DN uttryckte VDn Bordal att ansvaret för säkerheten delvis vilar på organisationerna själva. Hon betonade att det är upp till varje organisation att välja den nivå av säkerhet de vill ha från Tietoevry och att företaget levererar enligt den valda nivån:

> *Vi ska ge dem* (organisationerna) *support och vägledning: ”Vi tycker att ni ska köpa det här.” Men det är kunden som beslutar vilken nivå av säkerhet man väljer att lägga sig på. Det är ju en investering från kundens sida. [...] Du kan köpa en Rolls-Royce, eller du kan köpa en Skoda. Kunden måste själv*

> *bedöma utifrån sin verksamhet, hur kritisk är den? Nöjer jag mig med en Skoda som är säker och bra eller behöver jag Rolls-Royce?* (DN, 2024).

Kommentaren indikerar att Bordal anser att de drabbade organisationerna delvis har sig själva att skylla, eftersom de valt att teckna en billigare, mindre säker variant av Tietoevrys tjänst. Bland intressenterna finns det en splittrad syn på Bordals argument. Vissa kan hålla med om att organisationerna delvis bär ansvaret för den situation de befinner sig i, medan andra ser Bordals uttalande som ett försök att försöka avskriva Tietoevrys ansvar i frågan. Samtidigt finns det de som instämmer i att kunderna generellt sett får vad de betalar för och att det är viktigt att de drabbade organisationerna tar ansvar för sina egna val, inklusive de gällande säkerhetsfrågor. *[...]Däremot tycker jag hon har rätt i att kunderna får det de betalar för och just nu har många försökt köpa säkerhet utan att själva tänka* (Intressent 1, 2024, LinkedIn). Svaret på Bordals kommentar antyder att intressenten i denna kontext är överens och anser att organisationerna som köper tjänsten bör tilldelas ett större ansvar. Här verkar Tietoevrys svarsstrategi alltså varit framgångsrik, eftersom inget direkt ansvar tilldelas företaget av intressenten. Intressenten verkar istället skifta fokus till de drabbade organisationer som valt att inte köpa IT-skyddet med högst säkerhet.

En förklaring på detta skulle kunna vara det tidigare höga förtroendet för Tietoevry. Enligt tidigare forskning är det lättare för företag med starkt rykte att få positiv respons på sina svarsstaregier (Kholekile et al., 2018; Coombs, 1998). Samtidigt går det att argumentera för att de övervägande negativa reaktionerna innebär att detta inte kan vara fallet, och att det snarare kan bero på individuella erfarenheter hos de undersökta intressenterna. Enligt skyddsmotivationsteorin är intrapersonella egenskaper viktiga att ta hänsyn till för att förstå hur en individ uppfattar ett hot, och utifrån det agerar på det (Camerini et al., 2018). Mot den bakgrunden blir det viktigare att se till intressenternas individuella bakgrunder än till företagets tidigare rykte. Många av de intressenter som vi undersökt har en viss kunskap om IT-säkerhet och cyberattacker genom sina yrken, vilket kan göra dem mer benägna att ifrågasätta företagets oskuld och kräva ett mer proaktivt ansvarstagande.

Det finns också flera exempel på när intressenterna uttrycker en osäkerhet och tvetydighet kring attributet, där de både verkar förstå Bordals resonemang, men samtidigt menar att det kvarstår en förväntan om att leverantören ska leverera en viss standard av kvalitet och säkerhet.

> *Och det vilar massor av ansvar på den som köper tjänsten, formellt och juridiskt. Det jag tänker är att även om jag köper en Skoda förväntar jag mig en viss nivå av tillverkaren, inte att jag som beställare ska kravställa hela bilen och sedan få höra av säljaren att jag nog köpte fel* (Intressent 3, 2024, LinkedIn).

Här är det svårt att bedöma om svarsstrategin Bordal använt sig av har varit framgångsrik eller inte. Trots att intressenten uttrycker förståelse för det argument som presenterats, är den underliggande tonen ändå att Tietoevry bör ha ett övergripande ansvar. I förlängningen betonar citatet behovet av tillförlitlighet och förtroende mellan kund och leverantör. Kunden förväntar sig att företaget, oavsett om det är en bilproducent eller en IT-tjänsteleverantör, tar ansvar för kvaliteten och säkerheten hos den levererade produkten eller tjänsten. När detta förtroende ifrågasätts eller när leverantören försöker lägga över ansvaret på kunden kan det leda till förlorat förtroende och missnöje hos kunden, som verkar vara fallet för majoriteten av Tietoevrys intressenter.

5.5 Intressenternas uppfattade riskmedvetenhet

En viktig dimension i intressenternas reaktioner på cyberattacker är uppfattningen av hotets allvarlighetsgrad och/eller dess potentiella sårbarhet för den enskilda individen. Det eftersom det kan hjälpa oss förstå varför intressenterna reagerat som de gjort. Den generella tonen som går att uppfatta bland intressenternas kommentarer är att de ser mycket allvarligt på såväl krissituationen som på hur Tietoevry har valt att svara på den. Undertonen i flera kommentarer antyder att intressenterna ser på situationen som hotfull på både individ och samhällsnivå. *[…]ingen är säker, det är utgångspunkten* (Intressent 12, 2024, LinkedIn). Den tydliga betoningen på hotets allvar och den gemensamma sårbarheten i kommentaren indikerar att de ser situationen som mer än bara en isolerad händelse. Intressenterna tycks ha nått samma insikt som Bohlin, Sveriges minister för civilt försvar, att sådana attacker inte längre är sällsynta, utan snarare har blivit en ny normalitet. Det är därför viktigt att erkänna det hot de utgör. En intressent uttrycker det på följande sätt: *Cybersäkerhet är en av grundpelarna för vårt digitala samhälle och vi måste göra mer, vi måste bli bättre i denna domän* (Intressent 13, 2024, LinkedIn).

Denna typ av kommentar lyfter fram både den erkända allvarligheten i situationen och en stark uppmaning till handling, vilket indikerar en hög riskmedvetenhet (Rogers, 1983). Riskmedvetenheten går att tolka utifrån skyddsmotivationsteorin, där individens motivation att skydda sig ökar i relation till deras uppfattning om hotets allvar och deras egna sårbarhet (Rogers, 1983). Teorin lyfter att individers reaktioner och deras uppmaningar till åtgärder ses som ett resultat av en upplevd hotbild och en känsla av bristande kontroll över situationen. Det är något som belyses av en annan intressent: *Det är minst sagt oroväckande att så många regioner lider under enorma besparingskrav, vilket leder till att man inte anser sig ha råd att satsa på nödvändiga åtgärder gällande cybersäkerhet* (Intressent 14, 2024, LinkedIn). Intressentens kommentar illustrerar en rädsla för hur ekonomiska hinder inte bara ökar sårbarheten utan också försvårar en adekvat respons på denna typ av hot, vilket kan förstärka den upplevda allvarlighetsgraden och framkalla en känsla av frustration och hjälplöshet. Citatet exemplifierar en hög riskmedvetenhet, där intressenten inte bara ser hotet utan återigen uppmanar till konkreta åtgärder för att stärka cybersäkerheten. Tolkningen blir ännu mer betydelsefull när den jämförs med undersökningar som har visat en utbredd oro för säkerhet online bland svenskar, där cyberhot framträder som särskilt oroande (PwC, 2020). Trots att svenskar generellt är digitalt medvetna verkar det som att cyberattacker är något många känner sig hjälplösa och oroliga inför, både utifrån intressenternas reaktioner och de undersökningar som genomförts.

Samtidigt går det att urskilja ett mönster av missnöje som riktas mot Bordals kommunikation, där själva kommunikationen verkar utgöra hotet. *Tietoevrys vd visar här på en fullständig okunskap om förändringen och det är oroande* (Intressent 15, 2024, LinkedIn). Som tidigare adresserats i analysen har flera intressenter haft starka reaktioner på hur kommunikationen framställt händelsen på ett propagandaliknande sätt. I enlighet med PMT är det möjligt att identifiera en uppfattning hos intressenterna som återspeglar en sårbarhet gentemot den kommunikation som framförts av Bordal (Rogers, 1983). I förlängningen går det att identifiera ett samband mellan intressenternas reaktioner och den upplevda sårbarheten hos intressenterna, som inte bara ser en individuell hotbild utan en kollektiv hotbild på samhällsnivå som följd av det manipulativa språkbruket och bagatellisering av de problem som diskuteras. En annan intressent formulerar sin oro på följande sätt:

> *Vi kan inte låta sådana här ologiska uttryck för ansvarslöshet leta sig in i den allmänna diskursen som accepterade försvarstal. Vi pratar om en*

> *it-leverantör vars system hanterar en betydande del av den svenska befolkningens personliga data och informationsöverföringar* (Intressent 3, 2024, LinkedIn).

Intressenten uppfattar kommunikationen från Tietoevry som oacceptabel och potentiellt skadlig gentemot den svenska befolkningen. Skalan och omfattningen av hotet som kommuniceras av intressenten kan enligt PMT ligga till grund för hur intressentens relation formas, vilket i sin tur stärker argumentationen kring sambandet mellan uppfattad hotbild och attityd gentemot Tietoevrys kriskommunikation. Vidare går sambandet att jämföra med tidigare forskning som tydligt visar att krisen kan förvärras som ett resultat av att intressenternas perspektiv försummas (Pfeffer et al., 2014). I de exempel som presenteras ovan framgår det tydligt att intressenterna efterfrågar en kriskommunikation som är mindre bagatelliserande och förenklande än den som presenterades av Tietoevry. I förlängningen är det möjligt att argumentera för att krisen hade kunnat förminskats genom att öka förståelsen för intressenternas behov, uppfattning av hotbilden samt genom att tydligare anpassa kriskommunikationen gentemot intressenternas preferenser.

5.6 Intressenters förväntningar och känslomässiga respons

Det sista identifierade temat handlar om intressenternas förståelse, där två koder skapades som stöd för att kunna analysera det empiriska materialet; *inblick i intressenternas behov och förväntningar* samt *intressenters känslomässiga respons på företagets kommunikation.* Dessa koder är förankrade i den hermeneutiska traditionen genom att utforska både uttalande, och underliggande behov och förväntningar hos intressenterna (Prasad, 2018). I det empiriska materialet speglas detta i följande kommentar, där intressenten skriver:

> *Det är helt enkelt inte en hållbar situation för vårt samhälle. Vi måste göra både robusta och säkra lösningar tillgängliga och ändra det nuvarande rättsliga klimatet där det inte är ett alternativ att tala sanning på grund av de ekonomiska och juridiska konsekvenserna* (Intressent 16, 2024, LinkedIn, översättning min).

Intressenten uttrycker sitt missnöje med nuvarande praxis där den ekonomiska och juridiska faktorn tycks gå före ärlighet och säkerhet. Det kan tolkas som ett uttryck för en djup

frustration och ett behov av mer transparens och ansvarstagande agerande från företagets sida. Precis som Coombs (2023) menar, är intressenters förväntningar väsentliga för hur en organisation hanterar kriser. Förväntningarna intressenterna haft på företaget verkar inte ha mötts, vilket speglas tydligt bland intressenternas kommentarer. Intressentens 16 citat antyder också att kritiken inte bara riktas mot Tietoevry som enskilt företag utan också mot den övergripande samhällsstrukturen. Det indikerar att intressenten ser Tietoevrys situation som en del av ett större systemfel där företag inte tar tillräckligt ansvar för att skydda kundernas säkerhet och integritet. Det kan tolkas som ett uttryck för en önskan om förändring i samhället där företag och institutioner är mer transparenta, ansvarstagande och inriktade på att tillhandahålla robusta och säkra lösningar för allmänhetens bästa.

En återkommande trend bland kommentarerna är användningen av ord som *transparens, transparenta, transparent*. Det återspeglar ett behov och en förväntan från intressenterna om större öppenhet från organisationens sida. *Jag är en av de som blev påverkad av attacken och hade gärna fått mer information om hur och varför* (Intressent 17, 2024, LinkedIn). Citatet och de frekventa referenserna till transparens indikerar också på att det finns en upplevd brist på tydlighet och ärlighet i organisationens externa kriskommunikation. Undertonen i kommentaren kan tolkas som besviken snarare än argsint, vilket signalerar en stark önskan från intressenternas sida om en öppnare och mer ärlig kommunikation från organisationen. Enligt Syed (2019) och inom ramen av SCCT kan ett företags rykte definieras som uppfattningen av ett företags förmåga att leva upp till dess intressenters förväntningar. Här ser vi tydligt hur Tietoevry inte lever upp till de förväntningar som intressenten har. Som redan nämnts i analysen verkar det finnas ett gap mellan intressenternas och företagets uppfattning. Det tyder på att det föreligger klara brister i Tietoevrys förståelse för sina intressenter, vilket kan, och verkar ha, resulterat i felriktad kommunikation och därigenom minskat intressentförtroende.

Analysen av intressenternas känslomässiga respons avslöjar en tydlig och övervägande negativ ton i kommentarerna. Genom att granska kommentarsfältet kan vi se att majoriteten av det insamlade materialet är en reflektion av intressenternas egna känslomässiga reaktioner på företagets kommunikation efter cyberattacken. Forskning visar att sociala medier ger användare en plattform att uttrycka sina åsikter och känslor om organisationer i krissituationer (Oh et al., 2013; van der Meer & Verhoeven, 2013). Dessa uttryck av känslor på sociala medier kan skapa en negativ spiral som utgör en verklig risk för företagets rykte

(Pfeffer et al., 2014). Som redan framkommit i analysen finns det flera exempel på arga och tydligt upprörda kommentarer, och i kommentarerna kan man vid återkommande tillfällen urskilja en negativ ton gentemot företaget. Intressenterna beskriver både besvikelse och frustration. Samtidigt finns de intressenter som intar en starkt ironisk ton emot företagets kommunikation, exempelvis:

> *Vill gärna* 😂 *men precis som du säger, så vansinnigt ansvarslöst och bisarrt som det är, fastnar ju skrattet halvvägs…* 🤦‍♀️🤡 (Intressent 18, 2024, LinkedIn).

Citatet illustrerar en kombination av humor och besvikelse, vilket kan indikera en cynisk uppfattning av situationen och företaget. Den använda emojisarna, skratt-gubben och tjejen som håller för ansiktet, förstärker den känslomässiga tonen och ger intrycket av att kommentaren är både ironisk och nedslående. Humorn kan ses som ett sätt att hantera frustrationen över det upplevda 'ansvarslösa' och 'bisarra' beteendet från företaget. Samtidigt uttrycker kommentaren en viss förvirring och besvikelse över situationens allvar, vilket tyder på en känsla av förtroendeförlust gentemot företaget och dess kommunikation.

Många intressenter verkar inte dela samma humoristiska syn på situationen utan intar istället en strängare inställning gentemot företagets kommunikation. Ett exempel på detta är intressent 19, vars kommentar uttrycker en stark missnöjdhet: *Brist på respekt gentemot dina kunder att ta denna väg av förnekelse, är min åsikt. Väldigt konstigt minst sagt* (Intressent 19, 2024, LinkedIn, översättning min). Kommentaren reflekterar en stark uppfattning om brist på respekt gentemot företagets kunder. Vidare uttrycker kommentaren en känsla av förvåning och frustration över att företaget inte tar situationen på tillräckligt stort allvar. Det antyder att intressenten anser att företaget borde vara mer öppet och ärligt om den aktuella krisen, istället för att försöka bagatellisera eller förneka dess allvar.

Ytterligare ett exempel är: *Fatala fel i hela artikeln. Kan man något om säkerhet över huvud taget så vet man att alla har sårbarheter och brister, medvetna eller omedvetna. [...]* (Intressent 20, 2024, LinkedIn). Intressenten menar att kunskap om säkerhet innebär att man förstår att alla system, inklusive Tietoevrys, har sårbarheter och brister, oavsett om de är medvetna om dem eller inte. Undertonen i intressentens kommentar kan tolkas som ilska och förakt mot företagets påståenden om säkerhet. Denna kommentar antyder att intressenten har

en djupare förståelse för säkerhetsfrågor och att de inte accepterar företagets påståenden om att deras system är felfria. Som tidigare belysts i analysen är en god kommunikation, som innefattar transparens och öppenhet, viktigt för att intressenterna ska känna sig hörda. I takt med att digitala plattformar fortsätter att spela en allt större roll i hur information sköts och uppfattas, blir företagens förmåga att navigera i detta landskap allt viktigare (Pfeffer et al., 2014).

6. Diskussion och slutsats

Följande avsnitt ger en diskussion och slutsats om hur forskningen ger ny kunskap inom området strategisk kommunikation. Förslag på vidare forskning inom området intressenters reaktioner på kriskommunikation under cyberattacker i den digitala eran presenteras.

Syftet med studien var att bidra till forskningsfältet strategisk kommunikation genom att analysera intressenters reaktioner på Tietoevrys kriskommunikation efter cyberattacken. Detta har gjorts genom att besvara frågeställningarna;

1. *Hur uppfattar intressenter Tietoevrys externa kriskommunikation efter cyberattacken?*
2. *Och vilka underliggande budskap och teman framträder i intressenternas tolkningar?*

Det gick genomgående att observera att intressenterna delar uppfattningen om att Tietoevrys kriskommunikation har varit vag och otydlig. I våra 77 observationer fann vi ingen som värderade företagets kommunikation som bra efter cyberattacken. Många av intressenterna uppfattar Bordals uttalande som verklighetsförnekande där företaget undvek att ta ansvar för händelsen och valde att porträttera den som mindre allvarlig än den faktiskt var. Där kunde ett gap urskiljas mellan intressenternas och företagets uppfattningar. Intressenterna tillskrev företaget högt ansvar för cyberattacken medan företaget menade att det inte var deras fel. Diskrepansen mellan uppfattningarna verkade ligga till grund för intressenternas mycket upprörda reaktioner. Det kan indikera att SCCT-modellen inte är så effektiv som den tros vara, och att cyberattacker inte längre kan klassificeras in i offer-klustret.

Återkommande gick det att se en efterfrågan efter transparens och ärlighet av intressenter. Detta samspelar med tidigare forskning från Coombs och Holladay (2012) samt Wang och Hutchins (2018) om att uppfattningen av öppenhet under kriser är väsentligt för att upprätthålla förtroende under en kris. Genomgående i kommentarerna går det också att urskilja uttryck av misstycke som en del av en större bild, där intressenterna uppvisar en oro och ett missnöje över den nuvarande samhällssituation vi befinner oss i.

För att addera till kontexten har majoriteten av de intressenter vi undersökt en bakgrund inom IT, kommunikation eller liknande områden. Det gör att de besitter kunskap kring området som gör att deras reaktioner kan vara mer upprörda än hos en individ som inte besitter samma

kunskap. Eftersom LinkedIn är en plattform för yrkesverksamma kan det också vara fördelaktigt för intressenterna att kritisera Tietoevry för att framställa sig själva som kompetenta eller bättre. Ytterligare en förklaring på den övervägande negativa responsen skulle kunna vara den höga grad av hotbedömning som intressenterna verkar uppfatta. Samtliga intressenter verkar uppfatta cyberattacker som ett betydande hot både mot individen och samhället.

Vår studie blir ett viktigt bidrag för att förstå reaktioner hos intressenter i en svensk kontext. Det blev tydligt att intressenterna hade starka reaktioner på såväl krisen som kommunikationen, och deras åsikter verkar spegla de undersökningar som genomförts kring svenskarnas digitala uppfattningar. Vår studie bidrar således till att förstå kriskommunikation i en svensk kontext, och betonar vikten av att anpassa strategier till regionala förväntningar. Genom att fokusera på verkliga intressentreaktioner på LinkedIn, har vi gett praktiska insikter i hur kriskommunikationsstrategier tas emot av den avsedda målgruppen. Det dåliga mottagandet av Tietoevrys kommunikation kan vara ett resultat av bristen på intressenternas perspektiv och upplevelser, som vi i vår studie lyft.

Slutligen förbättrar denna studie vår förståelse av hur intressenter uppfattar och reagerar på kriskommunikation efter en cyberattack, och betonar behovet av transparens, snabba uppdateringar och kulturellt anpassade kommunikationsstrategier. Insikten om intressenternas perspektiv under kriskommunikationsframställning är inte bara relevant för praktiker som arbetar med krishantering, utan bidrar även med värdefull kunskap till den akademiska diskursen inom strategisk kommunikation.

6.1 Förslag på framtida forskning

Trots de insikter vi har fått, har vår studie vissa begränsningar, inklusive fokuset på endast ett företag och den specifika tidsramen. Framtida forskning bör överväga ett bredare spektrum av företag och förlänga tidsramen för att fånga långsiktiga trender i intressenternas reaktioner. Dessutom skulle det vara fördelaktigt att inkludera andra sociala medieplattformar för att jämföra tonen och innehållet i diskussioner över olika kanaler. Att undersöka effekten av olika kriskommunikationsstrategier på intressenternas förtroende och engagemang över tid skulle också ge värdefulla insikter för fältet strategisk kommunikation.

7. Referenslista

Böcker:

Björklund, M., & Paulsson, U. (2014). *Academic papers and theses: To write and present and to act as an opponent.* Lund: Studentlitteratur.

Coombs, W. T. (2023). *Ongoing Crisis Communication. Planning, managing, and responding* (4.). London: SAGE Publications.

Boréus, K., Bergström, G., & Björkvall, A. (Red.). (2017). *Textens mening och makt: Metodbok i samhällsvetenskaplig text- och diskursanaly*s (3:e uppl.). Studentlitteratur.

Bryman, A. (2008). *Samhällsvetenskapliga metoder* (2:a uppl.). Liber.78-91-47-09068-6

Flick, U. (2018). *The SAGE handbook of qualitative data collection.* London: SAGE.

Freeman, R. E. (1984). *Strategic Management: A Stakeholder Approach*. Pitman.

Gadamer, H.-G. (1997). *Sanning och metod (i urval)* (A. Melberg, Översättare). Daidalos. (Originalarbete publicerad 1960).

Guest, G., MacQueen, K. M., & Namey, E. E. (2012). *Applied thematic analysis*. Sage Publications.

Hallin, A., & Helin, J. (2018). *Intervjuer*. Studentlitteratur.

Heide, M., & Simonsson, C. (2016). *Krisen inifrån: Om organisationers krismedvetenhet.* Lund: Studentlitteratur.

Kvale, S., & Brinkmann, S. (2014). *Den kvalitativa forskningsintervjun (3:e uppl.).* Studentlitteratur.

Langemar, P. (2008). *Kvalitativ forskningsmetod i psykologi - att låta en värld öppna sig.* (2. uppl.). Stockholm: Liber.

Orwell, G. (2017). P*olitik och det engelska språket & därför skriver jag* [Politics and the English Language & Why I Write]. (R. Poirier Martinsson, Översättare). Stockholm: Timbro förlag.

Prasad, P. (2018). *Crafting Qualitative Research: Beyond Positivist Traditions*. New York: Routledge.

Schreier, M. (2012). *Qualitative Content Analysis in Practice*. SAGE Publications.

Sellnow, T.L., & Seeger, M.W. (2021). *Theorizing Crisis Communication* (2nd ed.). Chichester: Wiley Blackwell.

Silverman, D. (2022). *Doing qualitative research*. Los Angeles: SAGE.

Weiner, B. (1986). *An attributional theory of motivation and emotion*. New York: Springer.

Artiklar:

Avery E, Lariscy R, Kim S, Hocke T. A. (2010) Quantitative review of crisis communication research in public relations from 1991 to 2009. *Public Relat. Rev*. 2010;36:190–2 .

Cacciattolo, K. (2015). Defining organisational communication. *European Scientific Journal, 11(20), 79*. ISSN: 1857-7881 (Print), 1857-7431 (e-ISSN).

Camerini, A-L., Diviani, N., Fadda, M., Schulz, P.J. (2018) Using protection motivation theory to predict intention to adhere to official MMR vaccination recommendations in Switzerland, SSM - *Population Health, Volume 7, 2019,* 100321, ISSN 2352-8273,

Coombs, W. T. (1998). An analytic framework for Crisis Situations: Better Responses From a Better Understanding of the Situation. *Journal of Public relations Research.*

Coombs W. T. (2007). Protecting organization reputations during a crisis: the development and application of situational crisis communication theory. *Corporate Reputation Rev.* 2007;10:163–76 .

Coombs, W.T. & Holladay, S.J. (2012). The paracrisis: The challenges created by publicity managing crisis prevention. *Public Relations Review, 38(3)*, 408-415.

Harris, L., & Harrigan, P. (2015). Social Media in Politics: The Ultimate Voter Engagement Tool or Simply an Echo Chamber? *Journal of Political Marketing, 14(3)*, 251-283.

Kholekile, L., & Wang, J. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems, 35(2),* 683-714.

Kim, B., Johnson, K., & Park, S.-Y. (2017). Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity. *Cogent Business & Management, 4(1).* https://doi.org/10.1080/23311975.2017.1354525

O. Kulikova, R. Heil, J. van den Berg and W. Pieters. (2012) Cyber Crisis Management: A Decision-Support Framework for Disclosing Security Incident Information, 2012 *International Conference on Cyber Security, Alexandria, VA, USA, 2012*, pp. 103-112, doi:10.1109/CyberSecurity.2012.20.

Oh, O., Agrawal, M., Rao, H.R., (2013). Community intelligence and social media services: A rumor theoretic analysis of tweets during social crises. *MIS Quart. 37 (2),* 407–426.

Pfeffer, J., Zorbach, T., Carley, K.M., (2014). Understanding online firestorms: Negative word-of-mouth dynamics in social media networks. *J. Marketing Commun. 20* (1–2), 117–128.

Pourahmad, Z., & Hooshmand, R.-A. (2023). Smart Grid Protection Against Cyber-Attacks using PMUs and DC System Model. *In 2023 13th Smart Grid Conference (SGC)* (pp. 1-8). IEEE.

Tracy, S. J. (2010). Qualitative quality: Eight “big-tent” criteria for excellent qualitative research. *Qualitative Inquiry, 16*(10), 837-851.

Rogers, R. W. (1975) A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91(1)*, 93–114.

Rogers, R.W. (1983) Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation. *Cacioppo, J. and Petty, R., Eds., Social Psychophysiology, Guilford Press, New York,* 153-177

Spanos G, Angelis L. (2016) The impact of information security events to the stock market: a systematic literature review. *Computer Secur.* 2016;58:216–29 .

Syed, R. (2019). Enterprise reputation threats on social media: A case of data breach framing. *The Journal of Strategic Information Systems, 28(3),* 257–274.

Vance, A., Siponen, M., & Pahnila, S. (2012) Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management,* 49(3-4), 190–198.
Van der Meer, T.G., Verhoeven, P., (2013). Public framing organizational crisis situations: Social media versus news media. Public Relat. Rev. 39 (3), 229–231.

Wang, P., & Park, S.-A. (2017). Communication in Cybersecurity: A Public Communication Model for Business Data Breach Incident Handling. *Issues in Information Systems, 18(2)*, 136-147.

Wang, P, Johnson, C. (2018) Cybersecurity incident handling: a case study of the equifax data breach. *Issues Inf. Syst.* 2018;19:150–9 .

Yeom, S., Shin, D., & Shin, D. (2021). Scenario-based cyber attack·defense education system on virtual machines integrated by web technologies for protection of multimedia contents in a network. *Multimedia Tools and Applications: An International Journal, 80* (26-27), 34085-34101. Springer US.

Webbsidor:

Lindh, A., & Sundström, E. (2024). *Hackerattacken kan ta veckor att lösa – hundratals myndigheter och företag drabbade.* Aftonbladet. Hämtad från https://www.aftonbladet.se/nyheter/a/ab6Ek7/hackerattacken-100-tal-myndigheter-och-foretag-drabbade [16/4 -24]

Tidningen Näringslivet [TN]. (2023). *Företagen har svag beredskap mot cyberangrepp.* Hämtad från https://www.tn.se/article/27117/foretagen-har-svag-beredskap-mot-cyberangrepp/ [14/4 -24]

Cybersecurity and Infrastructure Security Agency. (u.å.). *Russia Cyber Threats Overview and adviosories.* Hämtad från https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia. [22/4 -24]

Dagens Nyheter. (11/02/2024). *Tietoevry efter attacken: Inga brister i vår IT-säkerhet.* Hämtad från https://www.dn.se/sverige/tietoevry-efter-attacken-inga-brister-i-var-it-sakerhet/ [15/4 -24]

Dagens nyheter (14/02-24). *20 år av data borta – hackarna kom åt säkerhetskopiorna.* DN. Hämtad från https://www.dn.se/sverige/20-ar-av-data-borta-hackarna-kom-at-sakerhetskopior/ [17/4 -24]

DIGG – Myndigheten för digital förvaltning. (n.d.). *Perspektiv på digitalisering utgåva 2* - Digital kompetens. Hämtad från https://www.digg.se/download/18.20e4ebeb18c4f70b1508826/1702995452733/Perspektiv%20pa%CC%8A%20digitalisering%20utga%CC%8Ava%202%20-%20Digital%20kompetens.pdf [10/4 -24]

E-Governance Academy, *National Cyber Security Index,* (2024). Hämtad från https://ncsi.ega.ee/ncsi-index/?order=-ncsi [02/03-24] [12/4 -24]

Europeiska kommissionen. (2023). *Digital Economy and Society Index (DESI)*. Hämtad från https://digital-strategy.ec.europa.eu/en/policies/desi [21/4 -24]

Göteborgsposten. (2023). *Digitaliseringen kan göra oss dummare.* Hämtad från https://www.gp.se/ledare/digitaliseringen-kan-gora-oss-dummare.14025183-b73d-4b44-b952-16f03dda6af1
[18/4 -24]

Myndigheten för samhällsskydd och beredskap [MSB]. (2024). *Antalet cyberattacker ökade kraftigt under 2023*. Hämtad från https://www.msb.se/sv/aktuellt/nyheter/2024/mars/antalet-cyberangrepp-okade-kraftigt-under-2023/ [19/4 -24]

Myndigheten för samhällsskydd och beredskap (MSB). (2024). *Cyberangrepp mot samhällsviktiga informationssystem – 25 rekommendationer för stärkt skydd mot cyberangrepp.* Publikationsnummer: MSB2287. Hämtad från https://rib.msb.se/filer/pdf/30558.pdf [16/4 -24]

Nationellt cybersäkerhetscenter. (2022). *Cybersäkerhet i Sverige 2022: Rekommenderade säkerhetsåtgärder (Rapport nr 2)*. https://www.ncsc.se/siteassets/publikationer/ncsc-rapport-2-cybersakerhet-i-sverige-2022-rekommenderade-sakerhetsatgarder.pdf [22/4 -24]

IBM Security. (2023). *Cost of a Data Breach Report 2023*. Hämtad från https://www.ibm.com/downloads/cas/E3G5JMBP [22/4 -24]

Internetstiftelsen. (2023). *Svenskarna och internet 2023.* Hämtad från https://www.svenskarnaochinternet.se [28/4 -24]

Office of the Australian Information Commissioner. (2023). *OAIC's summary of 7 ACT Directorates' data breach response plans*. Hämtad från: https://www.oaic.gov.au/privacy/privacy-assessments-and-decisions/privacy-assessments/oaics-summary-of-7-act-directorates-data-breach-response-plans [21/4 -24]

PwC. (2022). *Stor oro för cyberattacker bland svenska folket.* PwC Sverige. Hämtad från https://www.pwc.se/sv/pressrum/cyberhot-sverige.html [26/4 -24]

SVT Nyheter. (2024, 14 mars). *Antalet cyberattacker ökade kraftigt 2023.* Hämtad från https://www.svt.se/nyheter/inrikes/antalet-cyberangrepp-okade-kraftigt-2023 [12/4 -24]

SVT Nyheter. (25/01-24). *Vellinge kommun återgår till papper och penna efter hackerattacken* [Artikel]. Hämtad från: https://www.svt.se/nyheter/lokalt/skane/vellinge-kommun-atergar-till-papper-och-penna-efter-hackerattacken [22/4 -24]

Svenskt Näringsliv. (2016). *Företagen och digitaliseringen – om samhällsekonomiska effekter, kompetensförsörjning och nya regler för handel och personuppgiftsskydd*. Hämtad från https://www.svensktnaringsliv.se/bilder_och_dokument/mi6pm3_foretagen-o-digitaliseringen pdf_1007110.html/Fretagen+o+digitaliseringen.pdf [21/4 -24]

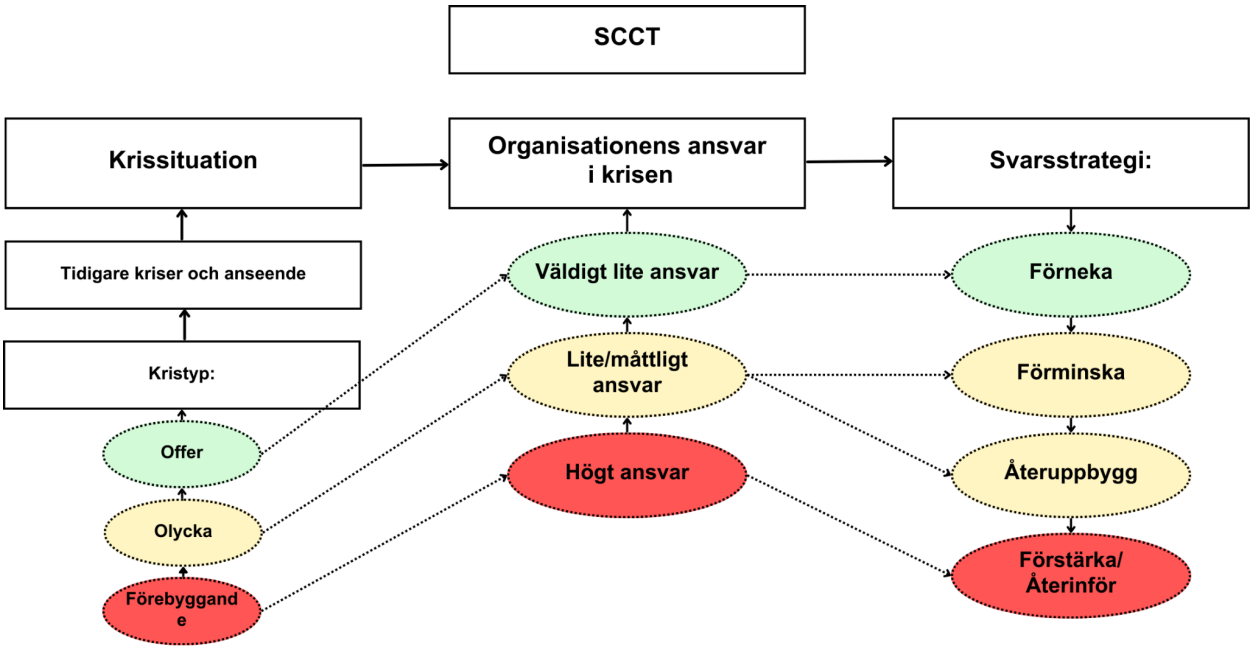
Tietoevry. (u.å.). *Om oss*. Hämtad från https://www.tietoevry.com/se/om-oss/om-tietoevry/ [10/4 -24]

Tietoevry. (2024, januari 25). *Det systematiska återställningsarbetet fortsätter efter ransomware-attacken – de första kundsystemen är igång igen.* https://www.tietoevry.com/se/nyhetsrum/alla-nyheter-och-pressmeddelanden/pressmeddelande/2024/01/tietoevry-det-systematiska-aterstallningsarbetet-fortsatter-efter-ransomware-attacken--de-forsta-kundsystemen-ar-igang/ [15/4 -24]

Tietoevry. (2021). *Ny mätning: TietoEVRY i topp bland svenska IT-leverantörer.* Hämtad från https://www.tietoevry.com/se/nyhetsrum/alla-nyheter-och-pressmeddelanden/ovriga-nyheter/2021/10/ny-matning-bland-svenska-it-leverantorer/ [21/4 -24]

8. Bilagor

Modell 1: SCCT- modellen, egen utarbetning.



Modell 2: Tidslinje över händelsen och inledande kommunikativa insatser från Tietoevry, egen utarbetning.

Tabell 1: Framarbetade teman och tillhörande koder, egen utarbetning.

Teman	Kod
Kriskommunikation	Vaghet och otydlighet i Tietoevrys kriskommunikation
	Kritik mot företagets kommunikativa hantering av attacken
Realism vs. framställning	Perceptionsgap: Finns det en märkbar skillnad mellan företagets framställning och intressenternas uppfattning av situationens realitet
	Förskönande av allvarliga incidenter
Ansvarstilldelning	Företaget bär huvudansvar för incidenten
	Företaget bär lite eller inget attribuerat till ansvar
Uppfattad allvarlighet och sårbarhet	Hög riskmedvetenhet: Intressenter känner en stark oro för potentiella eller faktiska risker som kommuniceras
	Låg riskmedvetenhet: Intressenter känner en minimal oro för potentiella eller faktiska risker som kommuniceras
Intressentanalys och förståelse	Inblick i intressenternas behov och förväntningar
	Intressenters känslomässiga respons på företagets berättelse

Utvalda citat från 20 intressenter:

Person	Yrke	Citat
Intressent 1	Cybersäkerhetingenjör	**Citat 1:** Det är tyvärr såhär kriskommunikation ser ut när krisen definieras som hotet mot varumärket och inte verkligheten. De blir medietränade och får superstrikta direktiv om vad de får lov att säga och inte. Såhär kan det inte få fortsätta. Det är ju direkt okunnigt att säga att man inte har några säkerhetshål. Det har de ju just visat att de hade. Och det är dessutom en utopi att tro att man är helt säker. Så varför måla upp en sån bild? Gammaldags. Däremot tycker jag hon har rätt i att kunderna får det de betalar för och just nu har många försökt köpa säkerhet utan att själva tänka. Det är svårt att upphandla, men att

		förstå skillnad på verklig backup eller spegling är inte så svårt. **Citat 2:** Det är tyvärr såhär kriskommunikation ser ut när krisen definieras som hotet mot varumärket och inte verkligheten. De blir medietränade och får superstrikta direktiv om vad de får lov att säga och inte. Såhär kan det inte få fortsätta. Det är ju direkt okunnigt att säga att man inte har några säkerhetshål. Det har de ju just visat att de hade. Och det är dessutom en utopi att tro att man är helt säker. Så varför måla upp en sån bild? Gammaldags. Däremot tycker jag hon har rätt i att kunderna får det de betalar för och just nu har många försökt köpa säkerhet utan att själva tänka. Det är svårt att upphandla, men att förstå skillnad på verklig backup eller spegling är inte så svårt.
Intressent 2	Säkerhetsspecialist	Alla kan bli drabbade av ransomware och jag är den förste som tycker det är viktigt att inte kritisera utan snarare uppmuntra och stötta så att vi vågar dela information och berätta om incidenter. Det är A och O för att vi ständigt kan bli bättre, minska risken för incidenter och minska deras konsekvenser. Men det är en katastrofal kriskommunikation att säga att de inte har några brister och att kunderna köpt för billiga tjänster samtidigt som man inte vet vad som hänt. Responsen på den här artikeln hade blivit helt annorlunda om hon sagt att vi analyserar och lär oss av detta för att ständigt bli bättre.
Intressent 3	Digital rådgivare	**Citat 1:** jag har läst DN:s intervju med Tietoevrys Sverigechef fyra eller fem gånger nu. Den känns inte på riktigt. Den är surrealistisk. Tietoevry vet inte något alls, inte en susning, om hur deras system har hackats. De vet bara att de själva garanterat inte har brustit i något led. Men angriparna har väl knappast tillämpat magi, försöker artikelförfattaren (NAMN) försiktigt framhärda: nog måste det funnits säkerhetshål? Det vet vi inte, menar Sverigechefen Venke, för Tietoevrys säkerhet är absolut tillräckligt hög.

		Vi lever i en tid med en amerikansk presidentkandidat som inte kan binda ihop två sammanhängande meningar men som journalister och experter ändå tvingas hantera på ett låtsat allvar. Jag menar inte att Tietoevrys hållning tas på allvar av DN. Men att den över huvud taget kan uttryckas på det här sättet är ett tecken i tiden. När makthavare börjar uttala sig tvärsäkert om sin egen skuldlöshet trots mängder av motbevis uppstår ett Orwellianskt språkbruk som får oss att ifrågasätta sanningen som väsen. Som får oss att tvivla på vår egen förmåga att förstå, då absurditeten är så uppenbar. Som konstform är denna nutidssurrealism otvivelaktigt kittlande, men som vägvisare för en mer rättvis värld direkt bedräglig. Vi kan inte låta sådana här ologiska uttryck för ansvarslöshet leta sig in i den allmänna diskursen som accepterade försvarstal. Vi pratar om en it-leverantör vars system hanterar en betydande del av den svenska befolkningens personliga data och informationsöverföringar. **Citat 2:** (NAMN), jag tycker absolut att dina tankar här är relevanta, inklusive hur det kan ha gått till. Och det vilar massor av ansvar på den som köper tjänsten, formellt och juridiskt. Det jag tänker är att även om jag köper en Skoda förväntar jag mig en viss nivå av tillverkaren, inte att jag som beställare ska kravställa hela bilen och sedan få höra av säljaren att jag nog köpte fel. Och ja jag triggades förstås av artikeln i sig, och frånvaron av att vilja erkänna någon form av brist i de egna leden, oavsett det handlar om den tekniska lösningen eller relationen till kunderna. Jag har under så många år hört så många ursäkter så jag lät den här historien klä skott för mer långtgående och bredare frustration. Dina tankar om frånvaro av vägledning för kravställning känns oerhört relevant och skulle förtjäna en egen djupdykning av journalistkåren. Skulle det vara okej att lägga till något om dina tankar om brister i segmentering som kommentar på blogg-inlägget? Kan ge relevanta perspektiv tänker jag.

Intressent 4	IT Arkitekt	Jag tolkade det också som ett försök på den typen av taktik av verklighetförnekande som politiker numer kommer undan med, att bara hävde en helt alternativ verklighet och sedan stenhårt hålla sig till den och inte låtsas om att den är helt påhittad. Frågan är hur man som IT-chef tror att man ska ha samma savant liknande magi som Trump har. Den här tekniken är nog svårare än man tror.
Intressent 5	Förvaltare	Nånannanismen vår tids största pandemi. Det är nån annans fel/skuld/ansvar mm. Aldrig mitt!
Intressent 6	Leveranschef	Jag tänkte exakt samma sak när jag läste den artikeln 😂 . "Vi har inte brustit i vår säkerhet" men ändå hackades ni i en av de största hackning attackerna i Sverige och det var ert system som gick ner... Hur kan man säga så ens?
Intressent 7	SQL Specialist (Structured Query Language/ programmering)	Affärsmässig mörkläggning! Det är sen gammalt.
Intressent 8	Informationssäkerhet	Hennes uttalande är ungefär lika motsägelsefullt som det gamla läkar-skämtet: "Operationen gick bra men patienten dog."
Intressent 9	Specialist inom cybersäkerhet	Jag höll idag en pressträff för att ge den senaste samlade lägesbilden av den cyberattack som drabbade Tietoevry för snart en vecka sedan och som därefter fått omfattande spridning i samhället. Kaskadeffekterna av attacken är stora och har spridit sig till företagets kunder och kunders kunder. I dagsläget är 120 myndigheter, ett antal kommuner och regioner samt ett antal privata företag drabbats. Vi befinner oss fortfarande i ett skede där fler kan komma att drabbas. Händelsen understryker vikten av den inriktning för det nationella cybersäkerhetsarbetet som regeringen påbörjade redan vid sitt tillträde. I december skärpte vi kraven på myndigheternas informations och cybersäkerhetsarbete genom förändrade eller uppdaterade regleringsbrev till ett hundratal myndigheter. Vi satsar i årets budget pengar för att kunna förstärka verksamheten vid CERT SE, och det

		pågår sedan förra våren ett arbete med att stöpa om det nationella cybersäkerhetscentret för att få bättre operativ förmåga i verksamheten. Utöver det pågår arbetet med en ny nationell cyberstrategi samtidigt som vi snart inviger ett nytt cybercampus på KTH, som en konsekvens av en budgetsatsning från regeringen. Detta för att få en bättre spetskompetensförsörjning i en sektor där behovet är stort och växande. Den senaste händelsen understryker hur angeläget det är för alla samhällsviktiga aktörer att ta sin cybersäkerhet på yttersta allvar och i detta kontinuerligt se över sina tredjepartsrisker. Utöver att bygga ett starkare eget skydd mot sårbarheter är det också uppenbart att man måste ha en fungerande kontinuitetsplanering som innehåller backup och återställningsfunktioner som gör att verksamheten snabbt kan komma upp på banan. Konsekvenserna av den nu aktuella cyberattacker är mycket allvarliga och det går ännu inte att överblicka hur långt den kommer att sprida sig. Det säkerhetspolitiska läget kräver att vi förstår att dessa sårbarheter måste tas på större allvar och det är bland annat mot denna bakgrund som regeringen tar ovan nämnda steg. Det räcker emellertid inte, kommuner och regioner har också anledning att prioritera frågan högre för att vi ska kunna bygga ett robustare samhälle.
Intressent 10	Data-management inom säkerhet	Är fortfarande chockad över hur man kan beskylla kunder för problem i miljöer man själv säljer och implementerar. Man kan inte droppa priserna och säkerheten för att vinna upphandlingar och sen säga att det är kundens fel
Intressent 11	Innovationsdesign	Det är ju bevisligen så att de åtgärder som fanns på plats inte räckte, att påstå något annat är direkt självmål. Och de av deras kunder som har möjligheten överväger nog att rösta med fötterna, sas, och byta leverantör.
Intressent 12	Coach inom informationssäkerhet och kriskommunikation	Kan verkligen hålla med om analysen, ingen är säker, det är utgångspunkten. Enda sättet är att kontinuerligt stärka sin förmåga att upptäcka, hantera och återställa. Lärandet en bärande del i att vår digitala resiliens - det är är vad vi jobbar med i Cyberly kluster och missionerar om i hela vårt nätverk. PS: med det uttalandet lägger man ansvaret på sina medarbetare. Skit bakom spakarna. Eller kunderna…

Intressent 13	Cybersäkerhetskonsult	Tack (NAMN) för uppenbart engagemang och påvisande av allvar i denna fråga! Cybersäkerhet är en av grundpelarna för vårt digitala samhälle och vi måste göra mer, vi måste bli bättre i denna domän. Jag tycker vi borde vara världsledande inom denna domän - vi har definitivt förmåga om detta görs på rätt sätt! Noterar att regeringen tar detta på största allvar, mycket gott betyg.
Intressent 14	Information och cybersäkerhet	Det är minst sagt oroväckande att så många regioner lider under enorma besparingskrav, vilket leder till att man inte anser sig ha råd att satsa på nödvändiga åtgärder gällande cybersäkerhet. Som minister måste man verkligen jobba i motvind när regeringen i stort i princip gör det omöjligt att förbättra säkerheten för våra regioner.
Intressent 15	Konsult inom internet arkitektur	Tror vi måste tolka detta som ett systemfel i IT-branchen. TietoEvry är ett exempel, men kunde det inte varit någon annan leverantör? EU har ju bestämt sig för att skydda kunderna och med lag skifta över mer ansvar på leverantören. Det är dags för alla, från företagsledningen och neråt att förstå att på grund av sådana här attityder mot säkerhet och kunder kommer dom att bli reglerade mer än förut. Det är dags att gå före och göra rätt för att bli marknadsledare i den reglerade marknaden. Tietoevrys vd visar här på en fullständig okunskap om förändringen och det är oroande
Intressent 16	Författare om samhället och säkerhet	Many times when It providers experience a breach and they either ignore to inform their customers or the market about it, or like in this case claims that they don’t have any weaknesses in their cyber security posture, it’s due to legal exposure and potential fines or sanction fees. It’s simply not a sustainable situation for our society. We need to make both robust and secure solutions available, and change the current legal climate where telling the truth is not an option because of the financial and legal consequences.
Intressent 17	Medieproducent	Bra skrivet! Jag är en av de som blev påverkad av attacken och hade gärna fått mer information om hur och varför. Hur de hanterar situationen inger inte direkt

		förtroende för dem som bolag kan man lätt säga.
Intressent 18	Företagsägare, kommunikation	Vill gärna 😂 men precis som du säger, så vansinnigt ansvarslöst och bisarrt som det är, fastnar ju skrattet halvvägs… 🤦‍♀️🤡
Intressent 19	Strategisk kundansvarig	Lack of respect towards your customers to take this path of denial, is my opinion. Very strange to say the least.
Intressent 20	IT Säkerhet	Fatala fel i hela artikeln. Kan man något om säkerhet överhuvudtaget så vet man att alla har sårbarheter och brister, medvetna eller omedvetna. Sen den etiska aspekten att beskylla kunder för att köpa osäkra lösningar av ens företag är inte charmig heller. Vem kommer lita på deras säljare igen?