# Cyberrisk

## Det aktuelle trusselsbillede og betydningen i bestyrelseslokalet

Jacobsgaard, Tom

# Cyberrisk: Det aktuelle trusselsbillede og betydningen i bestyrelseslokalet

**Cyber trusselsbilledet udvikler sig hele tiden. Hvordan ser det aktuelle og fremadrettede trusselsbillede ud, og hvilken betydning har dette for arbejdet i bestyrelseslokalerne? Det er to centrale spørgsmål, som denne artikel søger at besvare. Konklusionen er, at der er en kraftig stigning i omfanget og arten af cyberkriminalitet, og i hvor sofistikeret og professionelt de cyberkriminelle arbejder. Konklusionen på spørgsmål 2 er, at trusselsbilledet for den enkelte virksomhed er forbundet med virksomhedens strategi og forretningsmodel, og at cyberangreb kan medføre alvorlige og især for mindre virksomheder direkte livstruende konsekvenser. Cyberrisiko er således en forretningsmæssig risiko, der i allerhøjeste grad må tages alvorligt i bestyrelseslokalerne. En opfølgende artikel vil gå i dybden med overvejelser og beslutninger i bestyrelseslokalerne om cyberrisk.**

AF FORFATTER

**Tom Jacobsgaard**
Adjungeret professor, Center for Corporate Governance, Copenhagen Business School
E-mail: tj.ccg@cbs.dk

Tom var initiativtager til og direktør for Bestyrelsesforeningen og for CBS Bestyrelsesuddannelserne i årene 2013-2022. I perioden 2019-2023 var Tom ligeledes direktør for Bestyrelsesforeningens Center for Cyberkompetencer. Tom har mange års direktions- og bestyrelseserfaring.

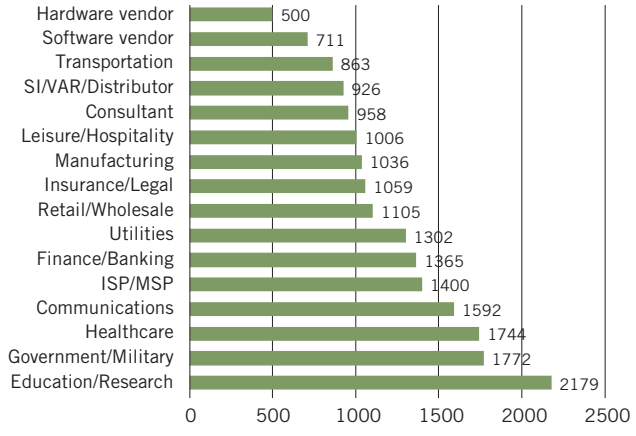
**Note:** En anonym referee takkes for en række kommentarer. Der gøres opmærksom på, at hensigten med de i artiklen udvalgte hændelser, data og beskrivelser er at give en beskrivelse af det overordnede cyber trusselsbillede, som virksomhederne er stillet overfor, og som bestyrelserne således skal være opmærksomme på. Formålet er således ikke at give en detaljeret og nuanceret beskrivelse af cyberkriminalitet, angrebsmetoder mv.

## Cyberangrebene bliver mere slagkraftige og hyppigere

Den 11. oktober 2023 bragte Reuters en artikel, hvor Google og Amazon udtaler, at de har klaret sig gennem internettets hidtil største DDoS (Distributed Denial of Service) angreb. Reuters artiklen refererer endvidere fra et blogindlæg, hvor Googles ejer, Alphabet Inc., orienterer om, at Google siden august 2023 har afpareret den ene lavine efter den anden af falske forespørgsler til virksomhedens servere. Cloudflare Inc., et ledende cybersikkerhedsfirma, der har bistået Google, udtaler, at angrebet var af en størrelsesorden, som "aldrig er blevet set før." Hundrede af millioner af falske forespørgsler i sekundet som gør det umuligt for legitim internet-trafik (medarbejdere, kunder, partnere, leverandører mv.) at komme igennem til hjemmesider, e-mail services, Teams, One Drive, data og applikationsservere mv. Deraf navnet DDoS som er en af mange angrebsformer, som hackere og de cyberkriminelle, private som statslige aktører, anvender.

Check Point Research (CPR)[1], der betragtes som en pålidelig kilde inden for cyber-intelligence, følger bl.a. udviklingen i ugentlige cyberangreb på virksomheder – per virksomhed, per industri og per geografi. Generelt bliver angrebene både mere slagkraftige, jf. ovenfor om Google og Amazon, men også hyppigere. Ifølge Check Point Research (2023) vil en virksomhed/organisation i gennemsnit have været udsat for cyberangreb 1.250 gange om ugen i 2. kvartal af 2023, hvilket er en stigning på ca. 10% over samme kvartal i 2022. Af Figur 1 fremgår det, at virksomheder og organisationer inden for uddannelse og forskning har været mest udsat de seneste år med flere end 2.000 angrebsforsøg om ugen efterfulgt af offentlige myndigheder og forsvaret samt sundhedssektoren.

**FIGUR 1: Antal ugentlige cyberangreb fordelt på industrier**



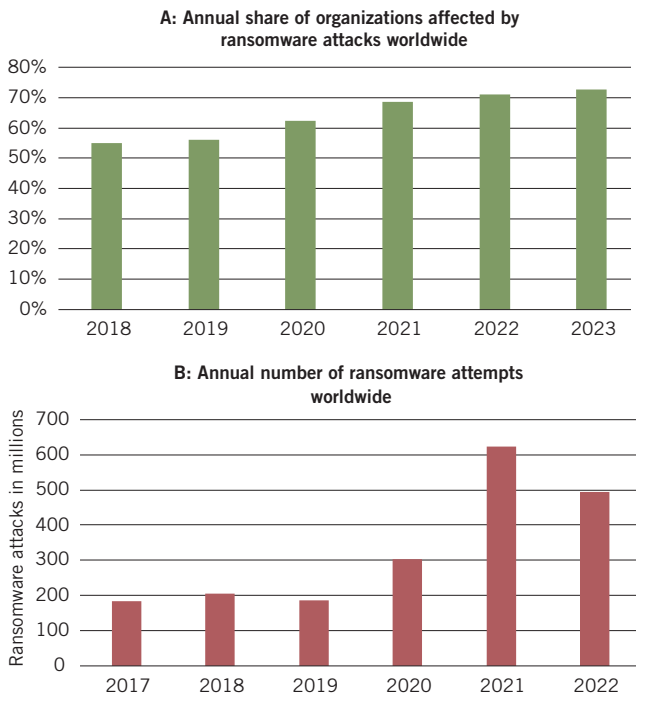

**Note:** Gennemsnitlig cyberangreb per uge per virksomhed i Q2 2023. Kilde: Check Point Research (2023).

## De dårligst beskyttede udsættes for flest cyberangreb

CPR fremhæver i sin analyse, at mange uddannelses- og forskningsinstitutioner, der under Covid-19 gik over til online learning platforms, var dårligt forberedt og derved åbnede en motorvej ind til institutionernes netværk, som hackerne let kunne infiltrere og udnytte med bl.a. ransomware[2] afpresning og tyveri af data. Uddannelsesinstitutioner er som udgangspunkt

1. *Check Point Research (*https://research.checkpoint.com/*) provides leading cyber threat intelligence to Check Point Software customers and the greater intelligence community. The research team collects and analyzes global cyber-attack data stored on ThreatCloud to keep hackers at bay, while ensuring all Check Point products are updated with the latest protections.*
2. *Ransomeware gør virksomhedens data og systemer utilgængelige, oftest ved kryptering. Virksomheden kan få de-krypteringsnøgle af hackerne ved at betale en løsesum.*

**FIGUR 2: Udvikling i ransomware angreb på globalt plan**




**Note:** A: Survery: 1,200 respondents; IT security professionals and practitioners; all from organizations with more than 500 employees. B: Data is based on SonicWall Capture Labs characteristics; wider industry metrics may vary. Kilde: A: CyberEdge/ Statista. B: SonicWall/Statista.

sårbare med et stort antal brugere, som anvender egne computere og tilsvarende devices, som ikke bruger VPN[3], og som tilgår internettet og derved institutionens netværk fra offentlige, ikke-sikrede wifi-net. Spørgsmålet er, om risiciene har været tilstrækkeligt erkendte og afvejet herunder om behovet for at beskytte den pågældende uddannelsesinstitutions egne data og kritiske systemer fx ved at etablere multifaktor login, segmenterede netværk og DMZ[4]?

Det fremgår også af Figur 1, at IT-hardware og software virksomheder relativt set har været udsat for markant færre cyberangreb end virksomheder i andre industrier. Det vil være en rimelig antagelse, at IT-virksomheder har større ledelsesmæssig opmærksomhed rettet mod cybertruslen såvel som kompetencer og kapacitet til at sikre netværk, servere og data mod cyberkriminelle, også når de angribes. Eksemplet ovenfor om det historisk store DDoS angreb mod Google og Amazon, som blev afvist, illustrerer denne kapacitet. Erfaringen blandt observatører af cyberkriminalitet er på linje med statistikken vist i Figur 1, at de cyberkriminelle generelt set vælger at prioritere angreb mod virksomheder, der er dårligst beskyttet.

## Mange former for cyberangreb

De cyberkriminelle optimerer og udvikler hele tiden arbejdsmetoder og angrebsformer, som det sker i enhver anden industri. Afhængig af grupperingsmetode og detaljeringsgrad kan angrebsformerne opdeles i 54, 17 eller 11 kategorier, hvor de hyppigst anvendte er phishing mails og ransomware. I 2022 blev der dagligt afsendt over 3 milliarder phishing mails (samt et ukendt antal *'smishing'* SMS angreb og *'vishing'* mobilopkald), hvor brugerne lokkes til at aktivere tilknyttet kode (malware) og/eller franarres personlige oplysninger, som de cyberkriminelle kan anvende senere til et angreb fx med ransomware. I 2022 er rapporteret 493 millioner ransomware angreb, og som det fremgår af Figur 2A og 2B, berørte angrebene flere end 70% af alle virksomheder og organisationer.

De nyeste analyser peger stort set alle på, at antallet af ransomware angreb i 2023 er steget markant i forhold til 2022, se bl.a. Zscaler (2023), og vil fortsætte med at stige hjulpet af de cyberkriminelles brug af AI.

Til sammenligning er der rapporteret[5] om 7,9 millioner registrerede DDoS angreb i første halvdel af 2023, hvilket er 31% over samme periode i 2022, og om forventninger til en fortsat stigning fremadrettet jf. bl.a. udviklingen i trusselsbilledet som følge af den geopolitiske situation i verden. For interesserede i de mere tekniske aspekter af de cyberkriminelles angrebsformer kan henvises til SimpliLearn.com (2023) og 17-punkts oversigten.[6]

I bestyrelseslokalerne er det afgørende at forstå og opbygge viden om, hvad de forskellige angrebsformer kan føre til af negative forretningsmæssige konsekvenser for virksomheden fx tyveri af IP-rettigheder og forretningshemmeligheder, tab af data henholdsvis manipulation af data, stop for forretningsaktiviteter, tab af omsætning og indtjening, forringet omdømme, kundeflugt, medarbejdermotivation, tab af konkurrenceevne, udbetaling af løsesum, svindel udbetalinger mv.

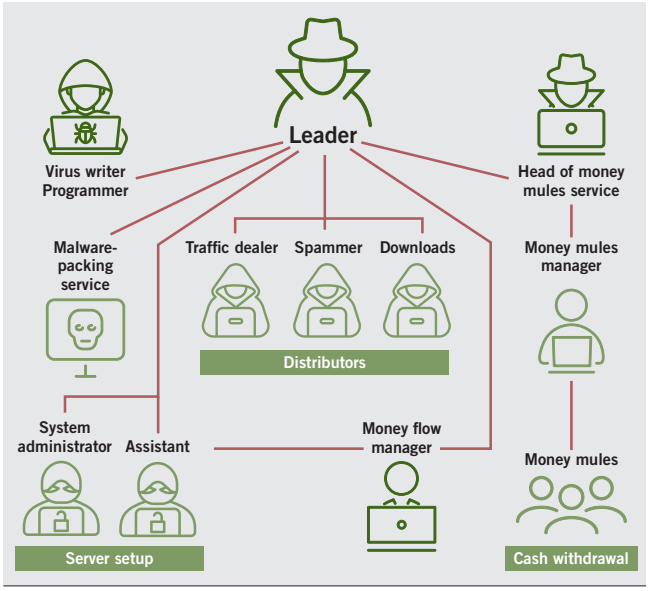
I den opfølgende artikel 2 vil vi gå dybere ind i overvejelser om omfang og sandsynlighed af konsekvenser ved cyberangreb bl.a. ved at anvende risk impact/risk probability modellen.

## Enheder på internettet scannes for sårbarhed og mål

De cyberkriminelle foretager eller får kollegaer i industrien til at foretage scanninger af alle enheder på internettet, bl.a. for at finde sårbarheder og mål for kommende cyberangreb. I foråret 2023 har Bestyrelsesforeningens Cyber Simulator Træningscenter på CBS monitoreret en server, som var sat op på internettet for at registrere omfang og art af scanninger, som en web-server eller tilsvarende enhed på internettet bliver genstand for. Monitoreringen viste, at den pågældende server blev scannet mellem 60.000 og 120.000 gange i døgnet.

3. *VPN står for virtuelt privat netværk – en tjeneste, der beskytter brugerens internetforbindelse og brugerens privatliv på nettet. VPN'er skaber en krypteret tunnel til brugerens data, beskytter brugerens onlineidentitet ved at skjule brugerens IP-adresse og giver brugeren mulighed for at bruge offentlige wi-fi-hotspots på sikker vis.*
4. *DMZ står for: Demilitarized zone er en zone som fungerer som en adskillelse mellem organisationens eksterne netværk (internettet) og det interne netværk (LAN).*
5. *https://cybermagazine.com/articles/global-events-driving-increase-in-ddos-attacks*
6. *Malware; Phishing, Man-in-the-middle, Distributed Denial of Service, SQL-injection, DNS-tunneling, Zero-day Backdoor, Password steal, Drive-by download, Cross-site scripting (XSS), Rootkits, DNS-spoofing, Internet of Things (IoT), Session hijacking, URL-manipulation, Cryptojacking, Insider.*

**FIGUR 3:** Organisering af cyberkriminalitet




## Professionalisering af organisation og arbejdsmetoder blandt de cyberkriminelle

Figur 3 forsøger at illustrere, at de cyberkriminelle har professionaliseret ledelse og organisation, og at industrien, som i andre industrier, har indført specialisering og arbejdsdeling og har opbygget værdikæder og markedspladser. Værktøj kan købes, scanninger og DDoS angreb kan bestilles, og ransomware klargjort til angreb i en virksomhed tilbydes til overtagelse, bl.a. på dark web.[7] CPR og andre professionelle iagttagere redegør i deres analyser for, at de cyberkriminelle har opbygget et økosystem af mindre, agile kriminelle grupper, der har til formål at øge effektivitet og udbytte af indsatsen. Nogle grupper har efter det oplyste ligefrem indført fast arbejdstid, løn, ferie mv.

Professionaliseringen synes også at gælde for produktudvikling, hvor de cyberkriminelle har udvidet scope for deres angreb til samarbejdsplatforme så som Slack, Teams, OneDrive and Google Drive. Platforme, hvor bl.a. hjemmearbejde (Work from Home) har medført større sårbarhed over for virksomhedsfortrolige og følsomme informationer, der deles på disse platforme.

## De cyberkriminelle har taget AI til sig

Der har siden 2016 været advaret om, at de cyberkriminelle var i gang med AI. Phishingmails er i dag ikke mere fyldt med stavefejl og ordstillinger, der vil advare den enkelte om ikke at klikke på et link eller et vedlagte dokument. AI har også gjort phishingmails mere og mere personificerede og konkrete i forhold til modtageren. Falske SMS-kampagner kan genereres på et øjeblik fra en AI platform, der for modtageren af beskeden får den til at virke meget troværdig.

Der er grund til at tro, at de cyberkriminelle i stigende omfang anvender AI i forberedelse og udførelse af deres angreb. Det tidligere omtalte DDoS angreb på Google og Amazon, verdens hidtil største angreb, har efter alt at dømme anvendt AI. Social engineering og Deepfake[8] kampagner kan bruges til at ramme virksomhederne på deres omdømme, som man allerede i dag kan konstatere anvendes i betydeligt omfang politisk.

## Statslige aktørers rolle inden for cyberkriminalitet

Forskellige statslige aktører spiller en rolle på flere niveauer inden for cyberkriminalitet. Dels beskytter nogle statslige aktører de cyberkriminelle mod det internationale samfunds politimyndigheder. Dels udfører de statslige aktører selv cyberkriminalitet, bl.a. i form af cyberspionage og ved DDoS angreb på kritisk infrastruktur.

Forsvarets Center for Cybersikkerhed vurderer i sin 2023 redegørelse, at truslen fra cyberspionage mod Danmark og danske organisationer og virksomheder særligt kommer fra "Rusland og Kina, og at begge stater har en betydelig kapacitet, som de bruger til at kompromittere ofre verden over med herunder i Danmark", jf. Forsvarets Center for Cybersikkerhed (2023).

## Geopolitiske konflikter påvirker cyberkriminalitet og cyber trusselsbilledet

De seneste års geopolitiske udvikling, primært med Ruslands krig i Ukraine og Kinas bestræbelser på at etablere en alliance i opposition til USAs og Vestens globalt orienterede verdensorden baseret på demokrati og friheds- og menneskerettigheder, markedsøkonomi og retssamfund, har øget og vurderes fremadrettet at ville øge trusselsniveauet og omfanget af cyberkriminalitet, cyberspionage og destruktive cyberangreb. Andre geopolitiske konflikter, senest Hamas' terrorangreb på Israel og den medfølgende tilspidsning af konfliktniveauet i hele Mellemøsten, vurderes ligeledes at øge omfanget af kriminel cyberaktivitet. Den geopolitiske udvikling medfører samtidigt en yderligere svækkelse for en effektiv politimæssig efterforskning og retsforfølgelse af cyberkriminelle på tværs af landegrænser.[9]

## Cyberkriminalitet er en lukrativ forretningsmodel

Cyberkriminalitet har vist sig at være en økonomisk attraktiv aktivitet med betydelige afkastmuligheder og meget lille risiko (for at blive pågrebet). En kombination som i sig selv vil tiltrække flere til området og derved øge aktiviteten. Indberetninger om betaling af ransom til 10 kendte grupper af kriminelle viser i Figur 4, at de tilsammen har haft en indtægt på USD 283 millioner.

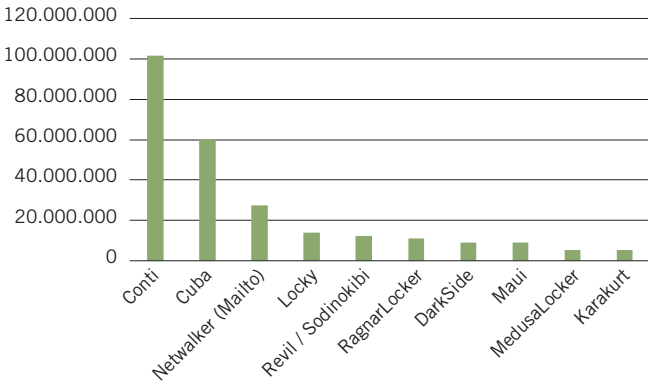
De cyberkriminelle har oprettet help-desks, som hjælper med instruktion om, hvordan virksomheden, som er offer for et ransomware angreb, betaler. Der kan også søges hjælp hos forsikringsselskaber og banker, jf. MacColl m.fl. (2023). I 2021

7. *Se eksempelvis* https://simplecode.dk/hvad-er-dark-web/ *for en beskrivelse af dark web.*

8. *Se bl.a. Berlingske Opinion s. 20 den 19.10.2023: Kunstig intelligens er en gamechanger for cybersikkerheden, Jeppe T. Jacobsen, Forsvarsakademiet og Mikael Ekman, Microsoft samt US NSA, FBI og CISA* https://media.defense.gov/2023/Sep/12/2003298925/-1/-1/0/CSI-DEEPFAKE-THREATS.PDF

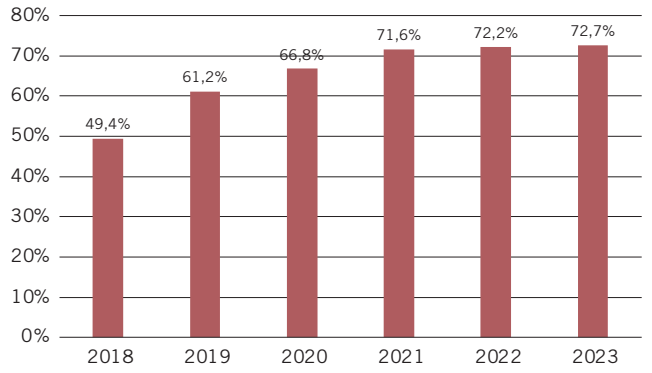
9. https://www.justice.gov/dag/page/file/1520341/download *US Department of Justice, Deputy Attorney Lisa O. Monaco – Comprehensive Cyber Review 2022, page 11-15; Interpol* https://www.interpol.int/Crimes/Cybercrime , https://www.interpol.int/News-and-Events/News/2023/Cybercrime-14-arrests-thousands-of-illicit-cyber-networks-disrupted-in-Africa-operation

**FIGUR 4: Samlede ransomware betalinger**




**Note:** Total payments in USD. Kilde: https://ransomwhe.re/. "Ransomwhere is the open, crowdsourced ransomware payment tracker."

**FIGUR 5: Andel af virksomheder der betalte ransom og fik leveret date tilbage**




**Note:** Online survey: 1,200 respondents; IT security professionals and practitioners; all from organizations with more than 500 employees. Kilde: CyberEdge/Statista.

faciliterede amerikanske banker mere end USD 1 milliard i ransomware relaterede betalinger, jf. CNBC (2022).

Ovenstående Figur 5 viser, at de cyberkriminelle i stigende og i overvejende grad leverer på troværdigheden i deres forretningsmodel om at levere data tilbage.

Hvor mange virksomheder, der faktisk betaler ransom, kan være vanskeligt at få belyst pga. issues i forhold til omdømme, firma politik og usikkerhed omkring lovlighed. Baseret på egne erfaringer er der betydelige kulturelle forskelle, hvor Danmark som udgangspunkt ligger lavt i tilbøjelighed til at betale sammenlignet med fx Sydøstasien og USA. Kvaliteten og hastigheden for at kunne genetablere data og systemer via back-up spiller en rolle for, hvor tilbøjelig en virksomhed kan være til at afvise betaling som en mulighed. Samme ræsonnement men med omvendt fortegn gælder for følsomheden af de data, som de cyberkriminelle måtte have stjålet og truer med at offentliggøre.

Veeam, der er et globalt firma inden for data beskyttelse og recovery (efter bl.a. ransomware angreb), har i 2023 offentliggjort en survey med 1.200 virksomheder, hvoraf tæt ved 80% svarede, at man havde betalt ransom for at stoppe et cyberangreb og/eller for at få data tilbage, jf. Veeam (2023). Det pågældende survey pegede også på, at 41% af virksomhederne, der faktisk betalte, havde en politik om ikke at betale!

Sammenfattende er der således en række forhold, man kan næsten sige på udbudssiden, der har medvirket til den stigende negative trend for cyber trusselsbilledet. En lukrativ forretningsmodel, professionalisering af ledelse, organisation og arbejdsdeling samt offensiv anvendelse af AI har øget kapaciteten og styrket effektiviteten i cyberkriminalitetsmiljøet. Dertil kommer den geopolitiske udvikling og de statslige aktørers rolle og øgede aktiviteter, der på længere sigt og for samfundet dog er den mest bekymrende udvikling.

## Trusselsbilledet og samfundets og virksomhedernes digitaliseringsgrad

Trusselsbilledet påvirkes naturligt også af den generelle digitaliseringsgrad i virksomheder og værdikæder og i samfundet som helhed. Danmark og danske virksomheder er helt fremme i førerfeltet på digitalisering og er senest i 2022 udnævnt som verdens mest konkurrencedygtige land, overordnet og i digital henseende, efterfulgt af Schweiz, Singapore, Sverige og USA, jf. IMDs World Competitiveness Index.[10]

Som udgangspunkt vil en højere digitaliseringsgrad i virksomheder og samfund øge sårbarheden, som man fx har set det ved tidlig anvendelse af IOT-komponenter med integration til virksomhedens netværk og systemer, og man så det ved eksplosionen i hjemmearbejde under Covid-19, der gav de cyberkriminelle mange, ikke-sikrede indgange til virksomheders og organisationers netværk. Denne sårbarhed var udtalt indtil der blev rettet opmærksomhed på problemerne og investeret i eftermontering af cybersikkerhed henholdsvis for fremadrettede projekter i cybersikkerhed by design og i etablering af økosystemer med samme høje niveau af cybersikkerhed, jf. også Damsgaard (2023).

NIS2[11] reguleringen har bl.a. til formål at etablere rammerne for økosystemer med fælles høje standarder til cybersikkerhed, der vil betyde, at Europa og europæiske virksomheder opnår en konkurrencefordel og reducerer risikoen for at blive angrebet af cyberkriminelle, private som statslige aktører, samt styrker evnen til at modgå de angreb, som rammer.

## En offensiv digital strategi integreret med cybersikkerhed

Tabel 1 synes at understøtte en hypotese om, at man kan være digital frontløber og samtidigt ved at integrere cybersikkerhed og cyberresilience i digitaliseringsstrategi og -projekter være relativt mindre attraktiv for cyberkriminelle at investere deres tid og anstrengelser på. I Q2 2023 var der i gennemsnit cirka 1.000 ugentlige cyberangreb for europæiske og amerikanske virksomheder, hvor det for afrikanske virksomheder var 2.164 angreb om ugen. Verdensbanken har gjort en række overvejelser om denne problemstilling, jf. World Bank (2022).

*10.* https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking.

*11. NIS2 er EU direktiv, jf.* https://digital-strategy.ec.europa.eu/da/policies/nis2-directive. *Direktivet er yderligere beskrevet i* https://kromannreumert.com/viden/artikler/nis2-eus-cybersikkerhedslovgivning-kritiske-vigtige-sektorer.

**TABEL 1: Udviklingen i antal ugentlige cyberangreb på virksomheder, inden for regioner**

| Region | Weekly Average of attacks per org | YoY Change |
|---|---|---|
| Africa | 2164 | 23% |
| APAC | 2046 | 22% |
| North America | 1011 | 18% |
| Latin Americas | 1745 | 9% |
| Europe | 1013 | 5% |

**Note:** Tabellen viser antallet af ugentlige angreb per organisation i Q2 2023 og angiver ændringen i procent i forhold til året før. Kilde: Check Point Research (2023).

Når en virksomhed henholdsvis en organisation bliver angrebet, vil de potentielle konsekvenser være større, jo mere digitaliseret virksomheden er. Der er flere data og IP-rettigheder, der kan stjæles, ødelægges eller offentliggøres. Der er større værdier, som kan gå tabt, og skader, som kan indtræffe, hvis der ikke betales ransom. Der er integrerede værdikæder, der kan sættes ud af spillet i dage, uger eller måneder, som det er sket for nogle af de største danske virksomheder såvel som for mange mindre virksomheder bl.a. hoteller, der blev overrasket over, at de var operationelt afhængige af en central IT-platform, som blev hacket.

Mens det oftest er de store virksomheder, der har de største økonomiske omkostninger, peger en analyse foretaget af Barracuda Networks[12] på, at 60 pct. af små- og mellemstore nordiske virksomheder, der bliver ramt af et alvorligt cyberangreb, må lukke deres forretning inden for seks måneder efter angrebet.

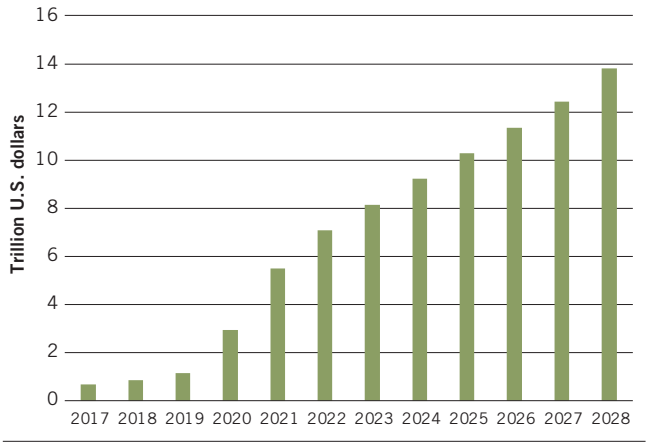
Det er en af artiklens hypoteser, at forskellen mellem større og mindre virksomheders og generelt mellem virksomheders evne til at overleve og komme videre efter et alvorligt cyberangreb skal søges i governance systemets fokus på resilience: Opbygning og træning af robusthed, modstandskraft og manøvredygtighed.

## 7.000.000.000.000 USD i årlige globale økonomiske implikationer

USD 7.000.000.000.000 (7 trillioner/på dansk 7 billioner) er de anslåede globale økonomiske implikationer, som i 2022 kunne relateres til cyberkriminalitet – og som det fremgår af Figur 6 i hastig vækst til anslået USD 14 trillion i 2028. USD 7 trillion svarer til den samlede børsværdi af Apple, Microsoft og Google (sept. 2023) og til 12 års omsætning i verdens største virksomhed målt på salg, Walmart Inc. Til sammenligning var det amerikanske BNP i 2022 på USD 25,5 trillion i 2022 og statsbudgettet for 2023 på USD 5,8 trillion. Det kinesiske ditto er på USD 4 trillion.

Perspektiveret i forhold til Danmarks størrelse i verdensøkonomien indikerer det økonomiske implikationer for danske virksomheder og for samfundet på et større 2-cifret milliardbeløb årligt (> DKK 50 mia.). Sammensat af driftstab knyttet til nedetid, tab af kunder og ordrer, omkostninger til genopretning, langsommere implementering af strategiske digitale projekter, ekstra investering i cybersikkerhed og cyberresilience, betaling

**FIGUR 6: Estimerede omkostninger ved cyberkriminalitet**




**Note:** Estimerede globale omkostninger ved cyberkriminalitet.
Kilde: Statista Technology Market Insights 2023.

af løsesummer for at få frigivet krypterede data, tab af data, tyveri af IP, brand og omdømme, medarbejdermotivation mv.

Hver femte danske virksomhed opgiver at have oplevet omkostninger og tab i forbindelse med cyberkriminalitet, jf. Deloitte (2023). Herhjemme har bl.a. Maersk, Demant og ISS i nævnte rækkefølge offentligt informeret om tab og omkostninger i milliardklassen. For en gennemsnitlig virksomhed henholdsvis organisation der bliver ramt af et alvorligt cyberangreb, anslås det, at den negative økonomiske konsekvens ligger mellem DKK 10 og 30 mio.

## Opprioritering af investering i cybersikkerhed

Virksomhederne har opprioriteret investeringer i cybersikkerhed fra ca. 12% af virksomhedens IT-budget i 2020 til ca. 24% i 2022, som det fremgår af Figur 7A. Digital transformation og cybersikkerhed er i dag de højest prioriterede investeringsområder i virksomhederne IT-budgetter. Også kapitalmarkederne har reageret på den stigende cybertrussel, som det fremgår af Figur 7B, med flere end 1.000 Investment deals i 2021 henholdsvis i 2022 og en samlet investering i årene 2018-2022 på USD 80 mia.

## Information om selskabernes cyberrisiko

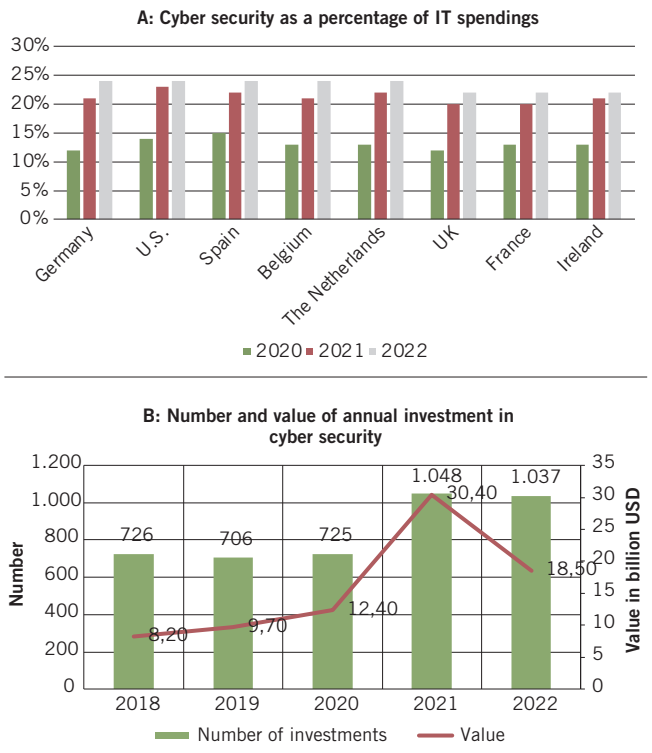
Visse globale virksomheder, som bl.a. Walmart Inc., har tillige valgt at offentliggøre omfattende og specifik information om selskabets cyberrisk til aktionærer og stakeholders og italesætte, at man anser selskabets cyberrisk som en systemisk risiko, Annual Report 2021, p. 18-19[13] (nedenfor i kort uddrag og oversat):

Vores compliance programmer, enterprise risk management processer og investeringer i nyeste informationsteknologi kan ikke eliminere alle systemiske risks knyttet til cyberrisiko. Disruption i vore systemer forårsaget af sikkerhedsbrister eller cyberangreb – inklusive angreb på vore forretningspartnere mv. – kan skade vores evne til at holde forretningen i gang, hvilket kan have en materiel påvirkning for os og kan resultere i tab, der

*12. https://assets.barracuda.com/assets/docs/dms/2023-email-security-trends.pdf*

*13. https://s201.q4cdn.com/262069030/files/doc_financials/2021/ar/WMT_2021_AnnualReport.pdf*

**FIGUR 7: Udgifter og investeringer i cyber-relateret IT**




**Note:** A: Based on a survey of executives, departmental heads, IT managers and other key professionals.
Kilde: A: Hiscox/Statista 2023. B: Momentum Cyber/Statista 2023.

kan få en materiel negativ påvirkning af vores finansielle situation, og/eller på vor indtjening, og/eller kan have en kaskade effekt, der negativt kan påvirke vore partnere, 3-parts service leverandører, kunder, finansielle partnere, og/eller andre 3-parties, som vi interagerer med på regulativ basis. I tillæg hertil vil sådanne sikkerhedsrelaterede begivenheder kunne blive bredt offentliggjort og skade vores omdømme hos kunder, partnere, leverandører, aktionærer, hvilket kan skade vores konkurrencesituation herunder særligt i forbindelse med vores e-commerce forretning, og som kan resultere i materiel reduktion i salg, negativ påvirkning af vores drift, salg, indtjening, finansielle position, cash flow og likviditet.

Ovenstående er helt i overensstemmelse med vurdering af udviklingen i de største risici, som virksomhederne står over for, jf. Tabel 2. Som eksempel angiver Allianz Risk Barometer 2023, at de højst rangerende risici er "Cyber incidents and Business interruption", jf. Allianz (2023).

Spørgsmålet er derfor, om danske virksomheder herunder også de mindre og mellemstore virksomheder i tilstrækkelig grad sikrer transparens til ejere og stakeholders om virksomhedens risikobillede og situation på cyberområdet, og om der ikke i større omfang med fordel kunne orienteres herom, fx i årsrapporter og ved generalforsamlinger.

For det første vil det skærpe opmærksomhed og viden i ledelsen (bestyrelse og direktion) om cyberområdet og derved styrke selskabets risikostyring af en af de væsentligste risici. For det andet vil det motivere til kompetenceudvikling fx uddannelse, nye kompetencer ind i bestyrelse og ledelse og ressourcepersoner.

For det tredje vil det være i overensstemmelse med god governance om at varetage selskabets interesse i dialog med ejerne i rollen som checks and balances funktion ift. selskabets risikoprofil og -appetit og i afvejning af tempoet i implementering af en offensiv digital strategi ift. hensyn til dataetik og -sikkerhed.

For det fjerde vil det fremme NIS2 målsætningen om at løfte cybersikkerhedsniveauet bredt i værdikæder og samfund.

## Bestyrelsen har ansvaret for selskabet, dets aktiver og værdiskabelse

Bestyrelsen er - af selskabets ejere og i henhold til selskabets vedtægter og lovgivningen - blevet betroet ansvaret for selskabet og dets aktiver. Det er i den forbindelse en særlig og ofte overset pointe, at bestyrelsen er et kollektiv, der har til opgave at varetage selskabets interesse.

Helt overordnet består opgaven, som bestyrelsen har ansvaret for (1) at passe på selskabets aktiver og (2) at skabe værdi på aktiver og forretningsplatform.

Det er temaet for en opfølgende artikel om cyber relaterede overvejelser og beslutninger i bestyrelseslokalerne om governance, strategi og værdiskabelse, risikostyring og resilience.

## Litteratur

– Allianz, 2023: *Allianz Risk Barometer 2023*. Rapport, 17. januar 2023.

FORTSÆTTER SIDE 35

**TABEL 2: Største risici for virksomheder Worldwide 2018-2023**

| Characteristic | 2018 | 2019 | 2020 | 2021 | 2022 | 2023 |
|---|---|---|---|---|---|---|
| Cyber incidents (e.g. cyber crime, malware/ransomware causing system downtime, data breaches, fines and penalties) | 40% | 37% | 39% | 40% | 44% | 34% |
| Business interruption (incl supply chain disruption) | 42% | 37% | 37% | 41% | 42% | 34% |
| Macroeconomic developments (e.g. inflation, deflation, monetary policies, austerity programs) | - | - | 11% | 13% | 11% | 25% |
| Energy crisis (e.g. supply shortage/outage, price fluctuations) | - | - | - | - | - | 22% |
| Changes in legislation and regulation (e.g. trade wars and tariffs, economic sanctions, protectionism, Euro-zone disintegration) | 21% | 27% | 27% | 19% | 19% | 19% |
| Natural catastrophes (e.g. storm, flood, earthquake, wildfire, extreme weather events) | 30% | 28% | 21% | 17% | 25% | 19% |
| Climate change (e.g. physical, operational and financial risks as a result of global warming) | 10% | 13% | 17% | 13% | 17% | 17% |

Note: 2,712 respondents; risk management experts from 94 countries and territories. Kilde: Allianz (2023) og Statista, 2023.