BOARD PERSPECTIVES

NO. 24/NOV. 2019
ISSN: 2246-6096

VELKOMMEN

TIL DANMARKS FREMMESTE BESTYRELSESPUBLIKATION

Board Perspectives - nyheder, tendenser og holdninger

INDHOLDSFORTEGNELSE

VELKOMMEN TIL BOARD PERSPECTIVES
Af Jakob Stengel - s. 2

WHY CYBERSECURITY IS ALSO A BOARD MATTER
Af Gert Hemmingsen & Jacob Herbst - s. 4

HVAD HOLDER DIG SØVNLØS? INTERVIEW MED PERNILLE FABRICIUS
Af Klaus Stubkjær Andersen - s. 8

NY UDDANNELSE FOR ERFARNE BESTYRELSESMEDLEMMER
Af Michael Monty - s. 10

HOW LONG HAS YOUR BOARD BEEN "THE FROG IN HOT WATER"?
Af Suzanne Jozefowicz - s. 12

CYBER - SECURE AND INSURE
Af Jens Houen Zakarias & Klaus Stubkjær Andersen - s. 15

CYBERSECURITY BØR FÅ ØGET FOKUS
Af Nikolaj Henum - s. 22

BOARD NETWORK

VELKOMMEN TIL BOARD PERSPECTIVES

- DANMARKS FREMMESTE BESTYRELSESPUBLIKATION

Velkommen til fireogtyvende nummer af Board Perspectives fra Board Network, The Danish Professional Directors Association. Board Perspectives henvender sig til alle, som interesserer sig for bestyrelsesagendaen i Danmark, og er den fremmeste, danske publikation med fokus på Corporate Governance og Board Leadership.

Board Perspectives udkommer kvartårligt – og byder i hvert nummer på en række artikler, skrevet af førende, eksterne eksperter samt interviews, nyheder og meget andet. Fokus er på indhold over form – og på nyhedsvinkler og holdninger med kant.

I dette nummer har vi fået bidrag fra Suzanne Josefowicz (Incorvus), Jesper Nytoft Bergmann (AVT), Jens Houen Zakarias og Klaus Stubkjær Andersen (begge fra RiskPoint), Pernille Fabricius (John Guest Group, Royal Greenland, MT Højgaard, Gabriel og Netcompany), Gert Hemmingsen (Valcon) og Jacob Herbst (Dubex) samt Steen Buchreitz Jensen (Scandinavian Executive Institute) og Stanislav Shekshnia (INSEAD).

Board's Role in Overseeing Cyber Risks

Virus, spyware. malware, hacking, blotlæggelse af data, crypto-locks og mange andre typer farer er i dag virkeligheden for alle virksomheder – men hvordan beskytter man sig bedst muligt? Hvad gør man i en krisesituation? Hvordan kommunikerer man om hændelsen til omverdenen? Og hvor er bestyrelsen i alt dette? Er ansvaret forankret i revisionsudvalget? Risikoudvalget? Hos hele bestyrelsen? Eller slet ikke – men snarere hos CEO, CIO, It-chefen eller hos eksterne partnere?

Kendte hændelser hos et utal af virksomheder fra Bahne over Demant og TDC til AP Møller–Mærsk har gjort, at de fleste er klar over, at risikoen eksisterer – men få ved, hvad de skal gøre ved det hos dem selv – og endnu færre får rent faktisk gjort noget inden de selv bliver ramt.

Vi har derfor fundet det rigtigt at sætte fokus på netop dette ved vores næstkommende medlemsmøde, som finder sted mandag d. 25. november kl. 13 - 18 under overskriften "Board's Role in Overseeing Cyber Risks".

Vi har endnu engang samlet et fantastisk panel fra både ind- og udland til at berette om deres førstehåndserfaringer – og til at give gode råd om håndteringen af disse risici.

- **Troels Ørting Jørgensen**, Chairman, World Economic Forum's Centre for Cyber Security, bestyrelsesmedlem i BLUEWALL og medlem af INTERPOLs Global Cybercrime Expert Group
- **Jukka Pertola**, Formand, TRYG, Siemens Gamesa Renewable Energy, GomSpace, IoT Denmark, Asetek, næstformand for COWI og bestyrelsesmedlem i Industriens Pension
- **Anne Louise Eberhard**, Bestyrelsesmedlem i FLSmidth, Topdanmark, Bavarian Nordic, Finansiel Stabilitet og Knud Højgaards Fond
- **Britta Dalunde**, Formand for Chorus, og bestyrelsesmedlem i Global Ports Investments Plc, ForSea, Arlandabanan Infrastructure og Projektengagemang.
- **Kim Schlyter**, Partner og Head of Cyber Risks Services, Deloitte
- **Morten von Seelen**, Senior Manager, Cyber Risks, Deloitte
- **Klaus Stubkjær Andersen**, Partner og Group Manager Liabilities, RiskPoint
- **Louise Knauer**, bestyrelsesmedlem i Solar og REKOM Group, samt tidl. Chief Information & Security Officer i TDC

ARRANGEMENTER FOR DET KOMMENDE ÅR

Vi er også stolte over vores kommende række af arrangementer i 2020 – med temaer som "Is There a New Ethical Reality for Boards?", "Board Composition and Succession", "Managing Reputational Risks" samt "Anchoring Strategy and Innovation at Board Level".

Vi glæder os til at se alle vore medlemmer igen – næste gang mandag d. 25. november kl. 13 – 18 i Deloitte Huset i København.

Hermed igen velkommen til fireogtyvende nummer af Board Perspectives. Rigtig god læselyst.

Jakob Stengel
Founder & Chairman

With everything from plumbing to heart surgery
you prefer dealing with someone who's an expert

Who do you rely on when it comes to
how your board is composed
and how its performance is evaluated?

Case Rose | InterSearch is the only
Executive Search firm in Denmark
to specialize in Board Search
and Board Evaluations

Because expertise matters!

CASE ROSE

INTERSEARCH

Global Executive Search & Leadership Consulting

Case Rose | InterSearch is the premier Copenhagen-based international retained executive search and leadership consulting firm. As part of InterSearch, one of the world's Top 10 executive search firms, we operate through an unparalleled global network of more than 95 corresponding offices in over 50 countries across the world. We specialize in finding Chairmen, Chief Executives, Finance and other Executive Directors, and Non-executive Directors. In addition, we provide clients with human capital solutions and leadership services, such as board evaluations, management appraisals, talent mappings, compensation benchmarks, onboarding advice, succession planning and executive coaching. Go to www.caserose.com or contact us at +45 21282882 / info@caserose.com.

WHY CYBERSECURITY IS ALSO A BOARD MATTER

Gert Hemmingsen
Senior Partner Valcon

Jacob Herbst
CTO Dubex

The threat is real. As companies and as private individuals, we are increasingly under cyberattacks, and the attackers are becoming more professional and efficient. A cyberattack can have a lot of consequences, both operational, legal and financial, and it is ultimately the board's responsibility to manage the risk of a cyberattack. Cybersecurity should be considered part of the general risk governance. The importance of cybersecurity has been emphasised by the major cyberattack on Maersk, which wiped out their entire IT infrastructure, and most recently by the attack on Demant. If it can happen to Maersk and Demant, it can happen to anyone.

What role should the board take?
We are not saying that you as a board member need to become the ultimate cybersecurity expert. But there is no doubt that the board has a responsibility to ensure that this topic is an integral part of the company's processes and risk governance.

It is important to understand that cybersecurity defences need to be layered and include a range of different measures, embracing technology solutions, user education and effective policies. There is no simple fix-all solution to cybersecurity, and it is a constantly evolving area requiring constant focus and attention.
So where to begin? Our recommendation would be to ensure that your board can check off the following four boxes in terms of cybersecurity: Understanding, Capabilities, Resources and Culture.

Understanding
For the board to understand the risk facing the business, you need to have sufficient insight into cybersecurity and the cybersecurity policies and procedures of the business to be able to ask qualified questions and understand the answers within these areas.

The board must understand how a cybersecurity incident can affect the business and thus ensure that the necessary contingency measures are in place. This requires basic understanding of the IT infrastructure and the cybersecurity posture beyond just being presented to some basic risk and efficiency metrics.

We would therefore recommend that you as the board ask the following questions of the organisation:

- What is the worst possible scenario for a cyberattack on us?
- Which GDPR-regulated data are we handling?

- What is our business continuity plan if a cyberattack eliminates the entire IT infrastructure?
- When was our incident response plan last tested?
- What were the learnings, and which changes and improvements were made after the test?

These questions should be asked of the people in the organisation who are directly responsible for these areas. In most cases, this will be the CIO and the CISO. But it is also important to get input from other relevant stakeholders, for instance the DPO or risk manager if such a role exists in your organisation.

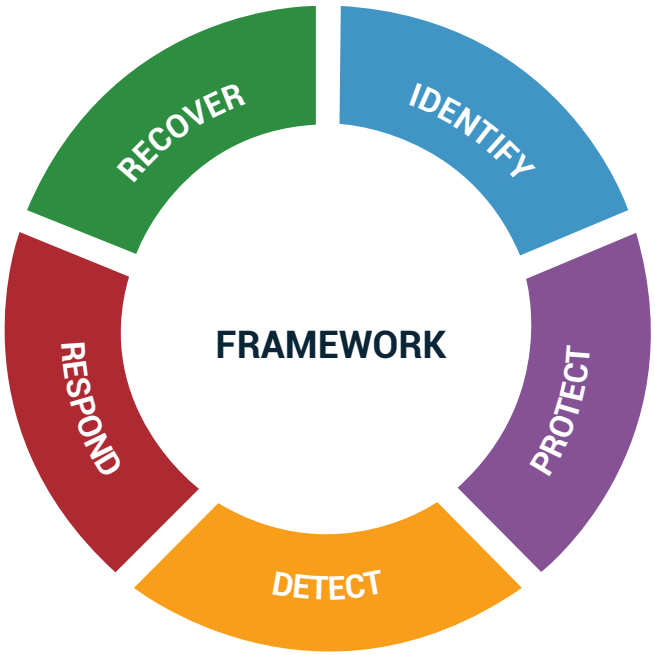
It may be necessary to look across the board composition to make sure that you have profiles with the required expertise to evaluate the adequacy of the responses to the above questions. You need to be able to verify that the company's risk governance applies to all aspects of the business, not just the IT department.

Capabilities

One way for the board to evaluate the company's cybersecurity posture is to consider the company's cybersecurity capabilities and readiness within the following areas as set out by the US National Institute of Standards and Technology Cybersecurity Framework. This framework identifies five overall cybersecurity functions that "represent the five primary pillars for a successful and holistic cybersecurity program". The framework can be applied by the board as a checklist to ensure that the organisation has a sufficient level of security in place.

The framework consists of the following five functions:

Figure 1: The five functions of NIST's Cybersecurity Framework (https://www.nist.gov/cyberframework/online-learning/five-functions)



In short, the framework aims to help companies verify that they have the necessary capabilities in place to handle all five aspects of a cyberattack. As the board, you have an obligation to ensure that the above capabilities within all five functions are in place. And if they are not, you should make it a priority for the executive team to get them in place. There are several other similar frameworks from other institutions, and they can be helpful as checklists in ensuring that your risk governance is up to speed.

Resources

However, getting the right capabilities in the organisation may be easier said than done. Cybersecurity resources and capabilities are in great demand, and it is difficult to get the right resources. And without access to cybersecurity resources, it is impossible to maintain the required level of preparedness and ability to execute within the organisation.

You need to ensure that the right resources are available to the organisation, either internally or via an external partner. Working with an external partner can often provide access to more specialised resources and competences, ensuring that the right resources are available at the right time. For each aspect of cybersecurity, the board should understand which resources are available and evaluate whether the competences and experience these individuals have match the requirements. For the board to understand the actual capabilities and resources in the organisation, you should ask specific questions such as:

- How many cybersecurity specialists do we have in the team?
- Who can we call for further help and assistance? And how fast can they help us?
- When was the last time we tested our readiness?

Culture

Last, but certainly not least, culture is a major success criterion for any company to achieve a successful cybersecurity programme. Security issues often occur because of the way users use the technology available to them. In most cases, this is not because the user has malicious intentions but simply because of ignorance or choosing the easy way in a busy workday.

To avoid this, it is important to establish a culture of security awareness. This is no simple task and usually requires quite a lot of work. It is therefore critical that both the board and the executive team lead the way by acting as role models, demonstrating constant focus on security and promoting and supporting a security-oriented culture.

[1] https://www.nist.gov/cyberframework/online-learning/five-functions

But to act as role models, you need to have an understanding of how cybersecurity works in practice as well as in-depth insight into the policies, procedures and processes in place throughout the organisation.

How do we start tomorrow?

By strengthening the focus on cybersecurity throughout the company with cross-functional cooperation, your company will also be able to optimise your value chain and achieve faster deployments, fewer reruns and consequently more satisfied customers in addition to strengthening your cybersecurity.

But it is a prerequisite that the entire company begins to think in terms of end-to-end processes from a security perspective. Not least the board.

Some board members would argue that cybersecurity is too technical and should therefore not be a board matter. However, with the right approach, we will argue that you can start improving your company's cybersecurity tomorrow.

Here is how you can begin:

- Together with your executive team, discuss and define how you can make cybersecurity an integral part of the business, and how you can think risk governance from an end-to-end perspective
- Decide on and communicate risk strategy and risk tolerance level on cybersecurity. How quickly do you want to be back in business? What can the employees do?
- Start the search for a board member with cybersecurity knowledge
- Ask for frequent reporting on attacks and the depth of these
- Seek sparring from other boards
- Consider taking more educational steps for the board on the topic

You can indeed start strengthening your cybersecurity tomorrow. Just be open to new ways of working and make sure that cybersecurity is an integral part of the company's risk governance. It should be incorporated in everything from digital solutions to cultural development.

BOARD NETWORK

Board Network – The Danish Professional Directors Association er Danmarks mest eksklusive bestyrelsesnetværk, og er det foretrukne forum for erfarne bestyrelses-medlemmer. Organisationens formål er at sætte fokus på Board Leadership samt at øge kendskabet til bestyrelsernes betydning for værdiskabelsen i og udviklingen af virksomhederne. Desuden uddeler Board Network den årlige hæderspris, The Corporate Governance Award, samt udgiver bestyrelsespublikationen, Board Perspectives hvert kvartal. For mere information, se www.boardnetwork.dk eller kontakt os på 21282882.

Vi tilbyder tre forskellige typer af medlemskab

- Personligt medlemskab – som giver adgang til alle vores arrangementer – DKK 12.000 excl. moms pr. år
- Corporate medlemskab – som giver adgang for to unavngivne medlemmer af virksomhedens ledelse / bestyrelse til alle vores arrangementer – DKK 24.000 excl. moms pr. år
- Den samlede bestyrelses medlemskab – som giver adgang for hele bestyrelsen til alle vores arrangementer – DKK 36.000 excl. moms pr. år

Lær fra de dygtigste. Netværk med de bedste.
BOARD NETWORK
The Danish Professional Directors Association
Det førende forum for erfarne bestyrelsesmedlemmer

HVAD HOLDER DIG SØVNLØS?
INTERVIEW MED PERNILLE FABRICIUS

Klaus Stubkjær Andersen
Group Liabilities manager i RiskPoint

RiskPoint er et partnerejet forsikringsagentur, der repræsenterer pt. 26 forsikringsselskaber, herunder flere Lloyds syndikater. RiskPoint har 110 ansatte fordelt på 9 kontorer i hhv. Danmark, Sverige, Norge, Finland, Tyskland, Schweiz, Holland, England og Spanien. Læs mere om RiskPoint på www.riskpoint.eu

Interview med **Pernille Fabricius**, Director og Group CFO John Guest Group og nuværende bestyrelsesmedlem i bl.a. NetCompany, MT Højgaard, Royal Greenland og Gabriel.

Spørgsmålene er stillet til Pernille Fabricius (PF) som privat person og svarene er udtryk for generelle holdninger og ikke konkrete i relation til Pernille Fabricius' bestyrelsesposter.

1) Hvordan forholder du dig til risici, både virksomhedens/ organisationens og dit personlige ansvar som leder?
PF: Som leder i en virksomhed er det naturligvis helt basalt vigtigt at forholde sig til hvilket niveau af risici, man er villig til at acceptere. Det er vigtigt at finde den rette balance og maksimere indtjening samtidig med at tab minimeres.
Personligt sørger jeg for at forstå eksempelvis hvad virksomheden tjener penge på (produkter, services, rådgivning m.m.), hvordan virksomheden drives (governance, politikker, procedurer m.v.), herunder hvilke systemer (IT og OT) er kritiske, samt geografisk udbredelse (omsætning, ansatte, produktion). Dette giver mig et indtryk af bredden og dybden af risici i pågældende virksomhed.

Det er vigtigt for mig, at risikostyring/-ledelse er tilpasset den konkrete virksomhed, dvs. at strategi, politikker, processer reflekterer de risici virksomheden står overfor.

I relation til det personlige ansvar fokuserer jeg på at forstå virksomhedens forretningsmodel som nævnt ovenfor.

I tillæg sikrer jeg mig at der er tegnet ledelsesansvarsforsikring.

2) Hvordan mener du at risk management bedst planlægges, organiseres og udøves i praksis?
PF: Risk management afhænger af virksomhedens situation, altså udviklingsstadie, markedsforhold, finansiering og organisering.
Generelt bør de væsentligste risici kortlægges af en risk management committee, baseret på løbende input fra organisationen. Bestyrelsen bør løbende holdes orienteret om status og udvikling heri.

Oftest anvendes en "Risk map" (koordinat med Impact (effekt) og Likelihood (relevans), Red.).

Det er vigtigt at være opmærksom på at risici ikke er statiske. Eksempelvis globale geopolitiske forandringer, så som Brexit og muligvis også af restriktioner i samhandlen på tværs af landegrænse; er under konstant forandring. Samtidig skal man kortlægge hvilke initiativer der sikrer, at virksomheden imødegår risici.

3) Hvorledes arbejder du med udvikling af risk management; giver best practice mening, eller er next practice mere relevant?
PF: På et årligt strategimøde ser vi på strategien i forhold til virksomhedens nuværende situation, sammenholdt med det øjebliksbillede vi har af virksomhedens risici. Vi spørger ligeledes os selv; hvilke risici ser vi idag og hvordan ser risici ud i morgen eller om 3-6-12 måneder. Vi tryktester naturligvis vores opfattelse af risici i organisationen samt involverer eventuelt også eksterne parter, om deres syn på risici.

Virksomhedernes risikobillede forandres med forskellig hastighed. Udviklingen gør, som drøftet tidligere, at strategien løbende må justeres.

Best practice er en udmærket tilgang i veletablerede brancher, hvor man anvender teknik og mekanik, der løbende optimeres uden at revolutioneres.

Next practice, altså anvendelse af nye metoder, giver rigtig god mening i brancher hvor produktudvikling er under konstant forandring, og man derfor ikke kan fortsætte med at gøre som hidtil, hvis man vil være markedsledende.
Jeg kan som eksempel nævne, at globale trends og tendenser, så som miljøvenlige materialer og socialt ansvar, nu indgår i drøftelser om udvikling af virksomheders produkter, altså at man kan genanvende og undgå forurening. Det kræver omstilling af hele forsyningskæden og produktionsudstyret,

hvilket betyder store investeringer, som ledelsen og bestyrelsen skal tage stilling til.

4) Hvad er i din optik de største risici for virksomheder og ledelserne lige nu, og kan risk management og forsikring imødegå disse risici i tilfredsstillende omfang?

PF: Den konkrete virksomheds risikobillede er individuelt, som vi drøftede tidligere.
Nogle risici er globale og generelle, og øver dermed indflydelse på alle virksomheder.

Jeg kan nævne et par for mig væsentlige og delvist uafklarede udfordringer :

- GDPR (General Data Protection Right, på dansk persondata-forordning, Red.): hvordan håndterer virksomheden data under de nye regler og regulering ? Manglende efterlevelse af reglerne kan resultere i bøder på op til 4% af virksomhedens globale omsætning. Samtidig betyder brud på reglerne ofte negativ omtale.

- Politiske forhold så som Brexit; Hvordan bliver påvirkningen af at England forlader EU; indkøb, produktion, omsætning, logistik, salgs-/leveringsbetingelser, ansættelseskontrakter, finansiering o.s.v.

Risk mapping kan som nævnt hjælpe til at få et overblik over risici og i den videre håndtering.

Jeg undersøger naturligvis også muligheder for at afdække risici via forsikring. Et eksempel herpå er Cyberforsikring. En Cyber forsikring kan dække erstatningskrav og omkostninger til afhjælpning og genopretning efter cyber hændelser. En Cyber forsikring kan også omfatte "forsikringsbare" bøder, men det er - så vidt jeg er orienteret - endnu uafklaret, om bøder der har et adfærdsregulerende element kan forsikres.

5) I hvilket omfang sætter lovgivning og regulering dagsorden for risk management?

PF: Det er en selvfølge at lovgivning og regulering iagttages og overholdes. Vi skal på godt dansk "have orden i penalhuset"!
I de virksomheder jeg er involveret i konsulteres rådgivere i det omfang vi er i tvivl om ny lovgivning og deraf afledte ændringer i regulering.

Konsekvenserne er, at virksomhederne må justere organisation, politikker og processer, med stigende omkostninger og kompleksitet til følge. Det er naturligvis ledelsens opgave ar sørge for, at ændringerne øver mindst mulig negativ indflydelse på effektivitet.
Udviklingen betyder nogen gange også at der er incitament og momentum til at få ryddet op i forældede systemer og bedagede processer.

6) Hvilken information om risk management og forsikring kunne være relevant for dig som leder, at få endnu bedre belyst?

PF: Vi konsulterer i forskelligt omfang rådgivere for at få opdateret information om risk management værktøjer og hvordan virksomheder bedst muligt kan forholde sig til risici.

Nye risici er som tidligere nævnt svære at få hænderne rundt om. Det kunne være interessant om rådgiverne udviklede værktøjer der kunne spotte nye trends og simulere effekterne af nye risici fx Cyber og Brexit. Jeg anerkender, at ingen endnu har opfundet en pålidelig krystalkugle der kan forudsige fremtiden, men med artificial intelligence og computer-/machine learning kunne vi måske komme et skridt nærmere?

Det vil også være relevant at samarbejde mere på tværs af virksomheder/bestyrelser for at udveksle erfaringer og lære af hinanden.

NY UDDANNELSE FOR ERFARNE BESTYRELSESMEDLEMMER

Af Michael Monty

Barren er sat højt på den nye bestyrelsesuddannelse, som Scandinavian Executive Institute i samarbejde med INSEAD skyder i gang i 2020 målrettet bestyrelsesformænd og bestyrelsesmedlemmer.

Navnet på uddannelsen er Advanced Board Programme, og CEO på Scandinavian Executive Institute Steen Buchreitz Jensen lægger ikke skjul på, at der er tale om en avanceret bestyrelsesuddannelse, der kræver, at man som deltager møder op med et højt vidensniveau og betydelig erfaring inden for bestyrelsesarbejde.

Stanislav Shekshnia

Steen Buchreitz Jensen

"Vi har gennem længere tid oplevet stor efterspørgsel på en bestyrelsesuddannelse på et særlig højt, fagligt niveau målrettet bestyrelsesformænd og bestyrelsesmedlemmer fra private virksomheder, offentlige institutioner og nonprofitorganisationer, som typisk har flere års relevant erfaring med i bagagen fra et antal bestyrelsesposter. Med Advanced Board Programme, som vi har udarbejdet sammen med INSEAD, er jeg sikker på, at vi fremover kan adressere den efterspørgsel og løfte i forvejen dygtige, erfarne bestyrelsesformænd og -medlemmer op til et endnu højere niveau i forhold til tankesæt og deltagernes konkrete, bestyrelsesfaglige kompetencer," siger Steen Buchreitz Jensen.

Første hold på Advanced Board Programme skal af sted til INSEAD i Frankrig i oktober 2020. Uddannelsen forløber over tre intensive dage på INSEAD under vingerne af uddannelsens programdirektør, Stanislav Shekshnia, der er Senior Affiliate Professor of Entrepreneurship and Family Enterprise på INSEAD.

Stanislav Shekshnia har i 10 år arbejdet som topleder og efterfølgende som iværksætter i Frankrig, USA, Rusland og Centraleuropa. Han har en kandidatgrad i økonomi, en Ph.d. fra Moskvas statsuniversitet og en MBA fra Northeastern University i Boston, og endvidere er han forfatter til en række bøger om ledelse og bestyrelsesarbejde.

"Advanced Board Programme er designet til folk, der allerede har en signifikant erfaring med bestyrelsesarbejde, som ønsker at udvikle sig og gerne vil arbejde med de særlige udfordringer, bestyrelser vil komme til at stå over for i de kommende år. Vi vil blandt andet dykke ned i, hvordan nye digitale teknologier vil influere på bestyrelsesarbejdet og drøfte, hvad det er for ny muligheder og udfordringer, som den digitale transformation indebærer," siger Stanislav Shekshnia.

Fokus på bæredygtighed

Et andet vigtigt tema for deltagerne på Advanced Board Programme bliver bæredygtighed og den position, som temaet allerede har og fremover vil få på bestyrelsernes agenda i Danmark og resten af verden.

Indsigt i, hvad ideen om bestyrelsesmedlemmers "uafhængighed" indebærer, er også et tungtvejende tema på uddannelsen.

"I øjeblikket taler man meget om bestyrelsesmedlemmers uafhængighed. Vi vil dykke ned i, hvad uafhængighed reelt betyder, og hvordan man som bestyrelse træffer uafhængige beslutninger. Vi vil derudover fokusere på formandsrollen: Hvordan bliver man en effektiv bestyrelsesformand, og hvilke specifikke kompetencer kræver det for at kunne skabe rammerne for et effektivt bestyrelsesarbejde," siger Stanislav Shekshnia.

Peer-to-peer diskussioner

Både Steen Buchreitz Jensen og Stanislav Shekshnia betoner betydningen af, at Advanced Board Programme giver god mulighed for peer-to-peer diskussioner, hvor kursisterne udveksler erfaringer og i høj grad skal lære af hinanden.

"Uddannelsen er baseret på, at deltagerne inspirerer hinanden og drøfter de udfordringer, som de hver især har i bestyrelsessammenhænge. Og når man sidder sammen med andre mennesker, der hver især kan bidrage med stor viden og mangeårige erfaringer, forventer vi, at det vil give brugbar videndeling på et særdeles højt niveau – samtidig med, at deltagerne forhåbentlig kommer hjem med nye, professionelle kontakter, som de efterfølgende kan udveksle erfaringer og netværke med," siger Steen Buchreitz Jensen.

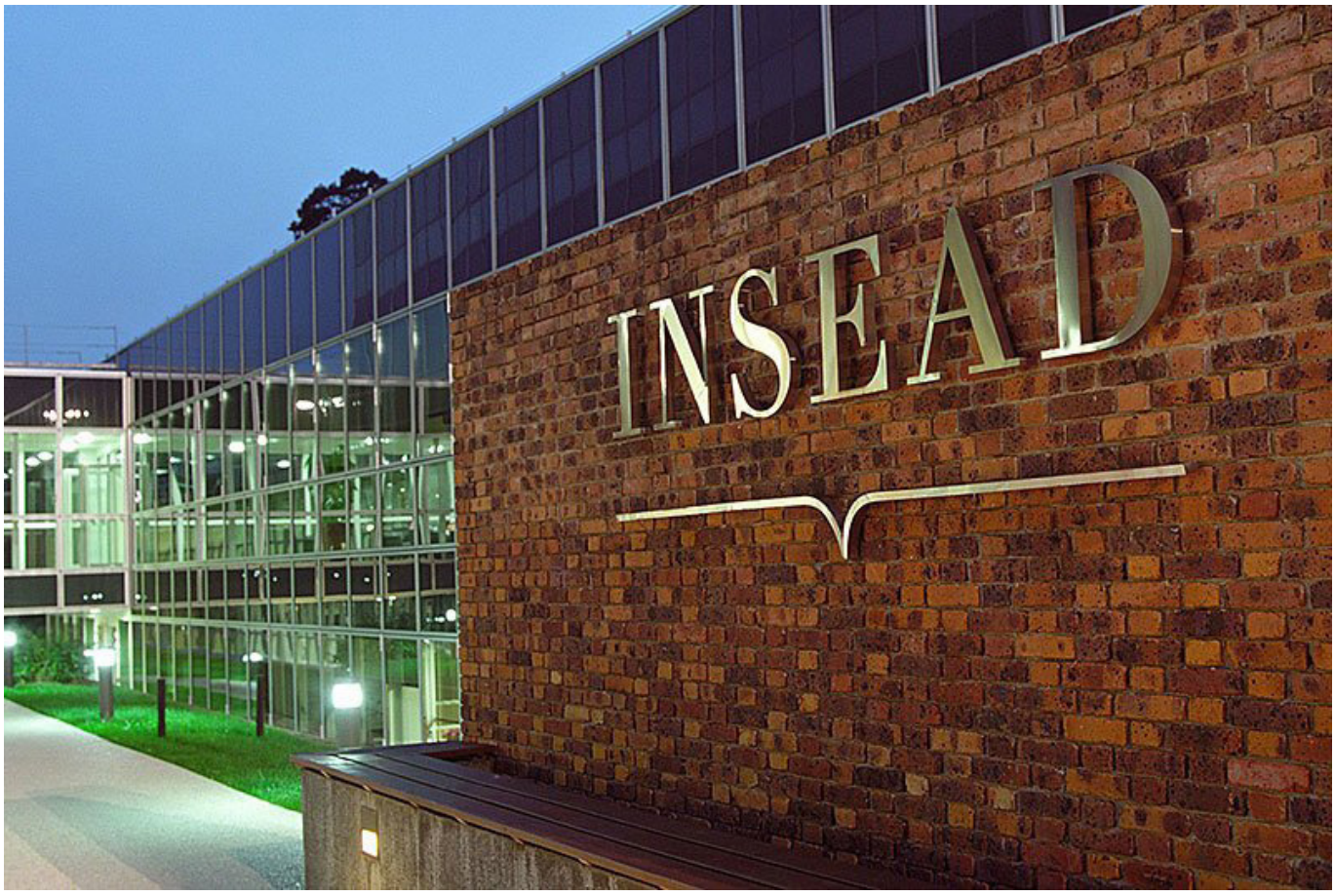
En del af undervisningen baseres på helt ny forskning og viden fra INSEAD´s fakultet, som endnu ikke er tilgængeligt for andre. "Uddannelsen vil adressere nogle af de issues, som vi mener er grundsten i bestyrelsesarbejdet i de kommende år, og de deltagende erfarne bestyrelsesmedlemmer vil komme hjem med nye kompetencer, nye ideer og ny viden," lyder løftet fra Stanislav Shekshnia.

UDBYTTE AF ADVANCED BOARD PROGRAMME

Programmet styrker dine bestyrelsesfaglige kompetencer og giver dig:

- Forståelse for det globale miljø, som din virksomhed opererer i, samt de trends, der vil påvirke dette miljø de kommende år.
- Viden om digitale teknologier og hvordan disse vil ændre bestyrelsens arbejde fremadrettet.
- Indsigt i hvad idéen om bestyrelsesmedlemmers "uafhængighed" indebærer samt hvordan det udleves.
- Ny indsigt i bestyrelsesformandens rolle og ikke mindst, hvordan man skaber rammerne for effektivt bestyrelsesarbejde.
- En oplevelse af udviklingen i franske ledelses- og governance-modeller.

Læs mere: https://www.se-institute.dk/uddannelser/advanced-board-programme/



HOW LONG HAS YOUR BOARD BEEN "THE FROG IN HOT WATER"?

By Suzanne Jozefowicz
CEO, Incorvus Ltd.

Introduction

The success enjoyed by digital leaders on the Nasdaq has eluded traditional boards who have been overtaken by the pace of technological advancement. They cling on to legacy thinking and greenlight so-called 'digital transformation' projects oblivious to the reality that their customers increasingly expect more and understand digital better than them!

For Incorvus, 'digital' is the use of data-centric technologies and implies complete metamorphosis – cultural, structural and procedural. Suzanne explains the immediate implications for boards, C-pop and recruitment as long-established brands disappear overnight – the latest, Mothercare.

Why do you imply boards have been like the proverbial "frog in hot water'?

It's been 15 years since Bezos first launched Amazon. Amazon exemplifies digital. It built its own digital platform to enable its business vision - so successfully the technology became a subsidiary in its own right – AWS.

AWS now dominates the global cloud market. You'd think boards would be saying "I'd like some of that!"

Not only does Amazon have a 15 year advantage, but because Bezos thinks digital, he is disrupting the concept of industry-specific markets too. What a digital organisation can do in one industry, it can do in another. Digital makes generic functions highly repurposable and therefore commercially advantageous.

What do you mean by 'digital'?

We define digital as "the use of data-centric technologies" – the capture, storage, management, retrieval, aggregation, processing, analysis, governance, description, manipulation, transmission and distribution of data. Systems and processes don't exist for their own sake – they exist to facilitate data, the data required or generated by the business! Digital puts data front and centre of any organisation. Data isn't an administrative detail – it's strategic!

If digital is 'all about data' why isn't it just an IT issue?

Research shows that organisations whose boards have a higher degree of digital 'savviness' than others, outperform the competition. There it is! Digital is a leadership Critical Success Factor.

Amazon is led by a digital native with his own technical advisor at board level and has a board structured around digital. Bezos didn't secure sustainable competitive advantage by decrementing digital as an IT issue. His success challenges boards to consider whether they can:

1. Lead on digital, if their customers outgun them on digital?
2. Mentor their executive, if they themselves need mentoring?
3. Assess candidates' capabilities, if they are not at least digital peers?
4. Choose digital advisors, if they cannot discern the quality of the advice?
5. Be diligent regarding business decisions, if they do not understand the strategic implications of digital to the same extent as their other fiduciary disciplines?

It could be argued that boards which cannot meet these tests, which devolves digital to IT or other subordinate functions, are in fact abrogating the entirety of their strategic and fiduciary responsibilities!

[1] Mothercare plc annual report and accounts 2016, Page 7. [2] Mothercare plc annual report and accounts 2019, Page 18.

Debenhams sought to bring in the right talent and even recruited their former CEO from Amazon.com but this failed as they transplanted the person but not the culture. The digital evangelist became the digital scapegoat, because the board wasn't really - 'onboard'!

Mothercare, now in administration, stated its strategy in 2016 was to become 'a digitally-led business". But there is little evidence to suggest they truly understood what this meant.

In 2016 Mothercare had trumpeted an augmented reality extension for its mobile app – a vanity marketing project. By 2019, it was forced to admit that "to grow our business, we needed to embrace developments in technology, however our current systems hamper our ability to do so. Additionally, our reliance on legacy systems results in a need to maintain knowledge of those systems." Again! Digital is about data! Why didn't Mothercare attend to their data in 2014 while they still had the budget?

Their Annual Report, admits honestly inter alia that a: "whilst the business had invested approximately a third of its fund raise in 2014 to play catch-up and to modernise its UK store base and its digital capabilities..... the difficult situation [has been] further fuelled by a fracture in the relationship between the non-executive and operating executives, a break-down in trust with key shareholders and the appointment of an array of increasingly expensive professional advisers."

Mothercare got other critical choices wrong resulting in: "Software impairment – £14.5 million. A charge of £14.5 million has been included for software impairment which comprises, £1.7 million licences for aspects of a planning system that will no longer be installed, and £12.8 million of general impairment against remaining intangibles."

Insolvency specialists simplistically attribute the demise of high street brands like Mothercare to the consumer cultural migration from bricks 'n mortar to "e-commerce". Mothercare might have a different view: "Firstly, as we closed stores we have lost the iPad generated sales from the store and the online sales in the catchment around the closure store have declined. The full price product online simply couldn't compete with the discounted clearance product in store." Now if they'd only been digital..... Sadly, Mothercare only realised the value of data and their need for data-centric systems in hindsight.

Organisational leaders in the 21st century need to understand why digital is a game changer, transforming not just businesses, but markets, governance, risk and opportunity. These are proper areas of responsibility for boards to consider, not matters to be delegated to subordinate opinion or IT. IT is there to enable board strategy, not to replace it.

That's where we are today. If you look forward to what Yuval Noah Harari has called 'the "Century of Algorithms", then the next challenge – but also opportunity – for boards, is successfully using AI - artificial intelligence (more accurately named 'augmented intelligence'). This won't be a case of boards simply announcing the latest fashionable experiment and waiting for the magic beanstalk to appear: it will be about the extent to which they and their organisations embrace data-centric thinking, and start to treat data with the respect it deserves. Their AI won't work without it.

How can Incorvus assist boards with digital?
Incorvus spans the fiduciary and technological divide.

Our team has blue chip experience of the traditional board disciplines – corporate finance, audit, treasury, risk, investment and management accounting – as well as having delivered the management information systems that gather, analyse, record, audit and present data to those functions and to the board.

We translate digital into terms that business will understand. We understand what the board and executive need to know and why, and how to make that happen – to help organisations become truly digital.

[3] Mothercare plc annual report and accounts 2019, Page 102. [4] Mothercare plc annual report and accounts 2019, Page 8.

LEARN FROM THE BEST

Board Mentors gives you access to the most renowned board directors and executives who have already done your job successfully.

Board Mentors matches executives and board directors with their more experienced colleagues. We match you with someone who has global best-in-class expertise and proven success in the specific area that you need help with here and now.

Through regular mentoring sessions, you get help solving your business challenges from someone who has done it successfully him- or herself.

Expect both personal and business growth.

Learn how we can match you with the right mentor. Contact us now.

Board Mentors
Board-mentors.com
info@board-mentors.com
Phone +45 2937 1733

BOARD MENTORS

CYBER - SECURE AND INSURE

Jens Houen Zakarias
RiskPoint.

Klaus Stubkjær Andersen
RiskPoint.

RiskPoint er et partnerejet forsikringsagentur, der repræsenterer pt. 26 forsikringsselskaber, herunder flere Lloyds syndikater. RiskPoint har 110 ansatte fordelt på 9 kontorer i hhv. Danmark, Sverige, Norge, Finland, Tyskland, Schweiz, Holland, England og Spanien. Læs mere om RiskPoint på www.riskpoint.eu

Cyber risici - hvad er det?
Cyber risici er i vores optik en bred betegnelse for de risici der eksisterer i - og transporteres via - computernetværk.

Cyber risici materialiserer sig i mange forskellige kombinationer under to hovedkategorier:

1. Uautoriserede personer har adgang til netværk og/eller data, uanset om sidstnævnte er beskyttede under lovgivning, eller;
2. Netværket kompromitteres og er utilgængeligt eller ikke anvendbart.

Vi bruger samlebetegnelsen Cyberhændelse om de forskellige kombinationsmuligheder.

Cyberhændelser er typisk kriminelle og strafbare, idet adgang til netværk og data ofte sker uden tilladelse eller mellemkomst fra dem der ejer eller kontrollerer netværket.

Cyber eksponering - hvilke trusler?
Det er offentligt kendt, at tre Nordisk domicilerede - alle børsnoterede og internationale aktiviteter - virksomheder har været udsat for Cyberangreb i de seneste par år. Angrebene har haft store negative konsekvenser for alle tre virksomheder. Kun to af virksomhederne har offentligt bekræftet at de var forsikret for (nogle af) tabene, som i alle tre tilfælde er anslået til at overstige DKK 500 mio..

Cyberangreb "version 1.0", karakteriseredes ved at virksomheder blev angrebet af hackere ved kampagner, hvor hackerne ikke identificerede konkrete ofre, men generelt afsøgte efter huller i sikringen af virksomheders netværk og ledte efter ofre som ikke var forberedt på angreb eller hvor forsvaret ikke var tilstrækkeligt til at modstå phishing, DDos, spyware og malware.

Cyberangreb "version 2.0" demonstrerer hvor sofistikerede hackerne efterhånden er blevet. Våbnene er stadig spyware og malware i kombination med ransomware.
Hackerne har erfaret, at ransomware er det mest effektive værktøj til at fravriste virksomheder penge, da ransomware rammer / lammer nerven (IT) i virksomheder, hvilket øger virksomhedens incitamentet til at betale.

Angrebene sendes ikke længere afsted som spredehagl, men er målrettede. Hackerne har skaffet sig adgang til, og spioneret i, de udvalgte virksomheders netværk i tilstrækkelig langt tid til, at de ved hvilke data og systemer de skal låse og kræver løsesum for at åbne adgang til igen. De dygtigste hackere infiltrerer også backup (i hvert fald de aktive, dvs. online, løsninger), og hvis der ikke findes hurtigt tilgængelige passive backups, så har virksomheden ikke anden udvej end at betale løsesum, hvis den vil have adgang igen.

Et ransomware angreb indebærer en anmodning om overførsel af midler. Løsesummen fastsættes ud fra en kalkule af hvad hackerne forventer at virksomheden kan betale; vi har til eksempel set, at løsesummen var samme beløb som direktørens bonus . Beløbene andrager ofte millioner kroner, og vi har set løsesummer på millioner dollars. Hackernes foretrukne betalingsmiddel er cryptovaluta.

Hackerne opererer med stigende professionalisme. Det er blevet en forretning at hacke og en god forretning forudsætter tilfredse kunder! Når virksomheden betaler løsesummen skal der låses op.

Professionalismen har betydet, at virksomheder i højere grad betaler løsesummen, fordi betalingen løser problemet.

Der er mindst to store udfordringer ved et krav om løsesum i cryptovaluta. For det første kræver det bådet tid og penge at få adgang til den ønskede cryptovaluta, og for det andet er der erfaringsmæssigt evidens for, at beløbet er til forhandling. Sådanne udfordringer kan løses af eksperter i forhandling af løsesum og konsulenter som allerede har cryptovaluta til rådighed. En Cyberforsikring kan dække både omkostninger til eksperter og betaling af løsesummen . Det er naturligvis en forudsætning for at indgå i forhandlinger om betaling af løsesum, at der er en begrundet formodning om at ransomware fjernes efter betaling, og at de samlede omkostninger ikke overstiger genetableringsomkostninger.

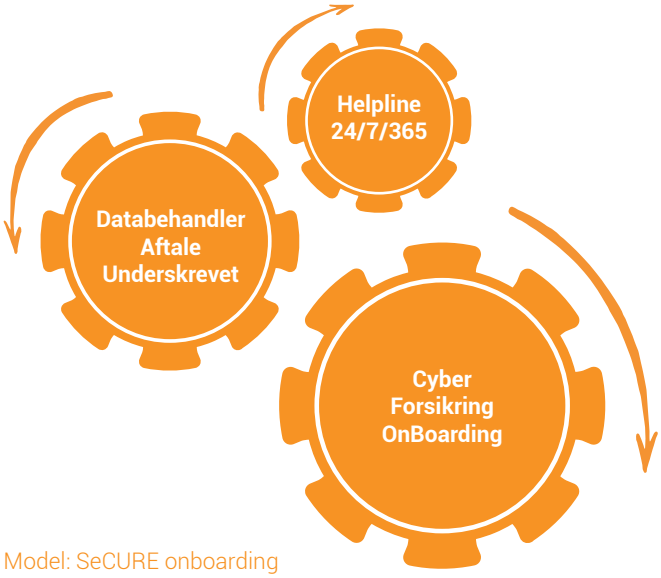
Udfordringerne er desværre ikke overstået efter at løsesummen er betalt, og nøglen til at låse data op er modtaget. Når adgang til netværk og data genetableres vil data sandsynligvis ikke findes i den orden de fandtes i forud for ransomware angrebet. Virksomheden må altså være forberedt på, at der vil være omkostninger forbundet med at genetablere og reorganisere data, filer og drev. Ud over omkostningerne må virksomheden indregne sandsynligheden for driftsforstyrrelser og eventuelt også et driftstab.

En Cyberforsikring kan dække både omkostninger til genetablering af data og driftstab som følge af et sikkerhedsbrist.

Cyberforsikring - hvad dækker den?
Cyberforsikring aktiveres ved at en cyberhændelse, som beskrevet i en eller flere af dækningsklausulerne materialiserer sig. De fleste Cyberforsikringer har i hovedtræk følgende tre dækninger med flere dækningsklausuler:

1. Erstatningsansvar og forsvarsomkostninger ved databrud og sikkerhedsbrist;
2. Omkostninger til beredskab i form af helpline, altså prioriteret adgang til rådgivning/service fra IT, PR og juridiske eksperter; Se nærmere i ISeCURE onboarding.
3. Tab af Indtjening og meromkostninger ved sikkerhedsbrist og administrative fejl og eventuelt også visse systemfejl.

Ikke alle Cyberhændelser er dækkede af en Cyber forsikring. Se nærmere i InSURE .
Generelt er cyberkriminalitet ikke undtaget, men hvis tabet resulterer i at penge overføres til utilsigtede personer eller at aktiver ødelægges, så er intentionen med Cyberforsikringen IKKE at erstatte pengene eller aktivet, for disse skal dækkes på separate forsikringstyper, henholdsvis Kriminalitetsforsikring og Bygning-/løsøreforsikring. Se nærmere herom sidst i artiklen.



Model: SeCURE onboarding

Intentionen bag en Cyberforsikringen er at refundere eller betale omkostninger til at identificere, stoppe, reducere, genetablere og reparere skader, der opstår ved forsøg på eller succesfuld indtrængen, og at betale dokumenteret tab af profit og eventuelle meromkostninger til at opretholde driften, samt at stille IT-, PR- og Legal helpline til rådighed. Se nærmere i SeCURE list.

Cyberforsikring kan også dække tab der er en direkte følge af den uautoriserede adgang til netværk og data; eksempelvis monetær og/eller "voucher" kompensation til de involverede personer plus omkostninger til fremtidig monitorering af kompromitterede kreditkort. I det omfang en bøde, fx GDPR/ Persondataforordning, er forsikringsbar, så kan sådanne bøder dækkes under en Cyberforsikring.

Fup og fakta om Cyberforsikring
Der har i efteråret 2019 været massiv mediedækning af cyber risici og Cyberforsikringer. I det følgende kommenterer vi nogle af de udsagn vi finder mest misvisende, og kommer med vores kommentar til forsikringsdækning af cyber risici.

"Lad være med at købe en forsikring, invester i stedet pengene i bedre sikkerhed"
Virksomheder må, hvis de er drevet med profit for øje, være interesserede i at drive en virksomhed med mindst mulig risiko, til lavest forsvarlige omkostninger og med maksimal gevinst. Det kræver risikostyring/-ledelse og heri indgår en analyse af, om det bedst kan betale sig at bruge penge på at sikre sig, eller om det er mere optimalt at forsikre sig.

I vores verden, forsikringsbranchen, går risk management og forsikring hånd-i-hånd. Virksomheder må i vores optik generelt sikre sig forud for at de forsikrer sig. Se nærmere i EnSURE.

DÆKNINGER I CYBERFORSIKRING

1) Erstatningsansvar og forsvarsomkostninger:
I. Ansvar for sikkerhedsbrist og persondatabrud
II. Myndighedskrav
III. Multimedie ansvar

2) Omkostninger:
I. Beredskab (IT, Jura og PR)
II. Afpresningsomkostninger inklusiv løsesum
III. Genskabelse af data

3) Tab af indtjening og meromkostninger:
I. Driftstab
II. Afledt driftstab fra IT-leverandører
III. Skade på omdømme

Driftstab omfatter tab af indtjening i den periode cyberhændelsen sker og meromkostninger under og efter. Skade på omdømme omfatter tab derudover, hvis forsikringstager mister yderligere indtjening efterfølgende grundet negativ medieomtale osv.

RiskPoints Cyberforsikring indeholder ikke sikkerhedsforskrifter. Vi vurderer risikoen på baggrund af den information, vi modtager ved indtegningen. Efterfølgende vil vi ikke begrænse dækningen yderligere end reglerne i Forsikringsaftaleloven.

Model: InSURE

Konkret i relation til IT og OT sikkerhed er dilemmaet altså ikke: "IT -og OT sikkerhed eller forsikring"?

Informationsteknologi (IT) og operationsteknologi (OT) er essentielle komponenter i de fleste virksomheders daglige drift.

Virksomheder investerer i IT -og OT sikkerhed, fordi de ikke ønsker at få kompromitteret deres konfidentialitet og integritet eller at få forstyrret deres drift.

Det er ikke muligt at sikre en virksomhed 100 % mod at blive kompromitteret på IT sikkerhed! Hvis virksomheden ikke vil bære den risiko alene, så er Cyberforsikring relevant.

Cyberforsikring tegnes af virksomheder, der på trods af deres sikkerhedstiltag ønsker at transportere den residuelle risiko til et forsikringsselskab. Jo bedre IT – og OT sikkerhed en virksomhed har, des lavere må risici være og deraf følger – alt andet lige – lavere forsikringspræmie. Forsikringspræmien fastsættes med udgangspunkt i risici, og varierer derudover alt afhængigt af forsikringssum og selvrisikobeløb.

"IT er outsourcet, så vi har ingen (cyber)risiko"
De fleste virksomheder har outsourcet hele eller dele af deres IT. Outsourcing indebærer, at en ekstern part tilbyder hardware, software og/eller håndtering af virksomhedens data.

Outsourcing har flere fordele, fx professionel og (omkostnings) effektiv håndtering af IT.

Virksomheder kan som nævnt ovenfor ikke sikre sig 100 % mod sikkerhedsbrist, og det kan outsourcing virksomheder heller ikke!

Risici forbundet med opgaver der outsources forskydes til outsourcing virksomheden, fx risiko for uautoriseret offentliggørelse af persondata eller fortrolige informationer og risiko for nedetid, der på påvirker driften af både IT og OT. Hvem der bærer ansvaret for at risici materialiserer sig i et tab afhænger af kontrakten mellem virksomheden der outsourcer og outsourcing virksomheden?

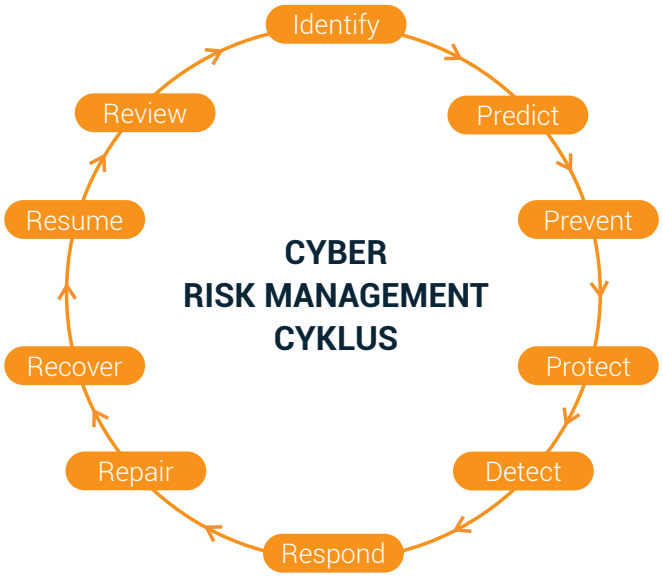
Outsourcing virksomheden er som udgangspunkt ansvarlig for fejl og mangler ved deres services, men vi har set eksempler på, at outsourcing virksomheden helt fraskriver sig ansvar for ovenstående situationer.

Hvis outsourcing virksomheden ikke kompenserer for ovennævnte tab, så står virksomheden tilbage med tabet. Disse tab kan dækkes af en Cyberforsikring.

SPØRGSMÅL VED CYBERHÆNDELSE

1. When the incident occurred
2. How and when the incident was discovered
3. The locations/offices affected
4. Whether the event involves any personal identifiable data
5. If so what is the data and what personal information does it include
6. How many records have been affected
7. Whether the affected data subjects are aware of the data breach
8. Whether any third parties are aware of the incident and, if so, how.
9. Whether the incident is having a direct impact on the Insured's ability to trade and generate income
10. Whether there is there a data breach response plan in place
11. What action been taken to minimise or mitigate the impact of the incident

Model: SeCURE list



Model: EnSURE cycle

Mht. uautoriseret offentliggørelse af persondata eller fortrolige informationer skelnes der i forsikringsdækningen ikke mellem hvor følsomme persondata lagres (databehandler), men, alene hvem der har indsamlet (dataansvarlige) de pågældende (person)data. Virksomheder er ansvarlige for følsomme persondata når sådanne data indsamles, og dermed også når sådanne data lækkes, hvilket forsikringsdækningen tager højde for.
Mht. risikoen for nedetid der påvirker driften, kan der tilkøbes udvidet dækning for driftstab som følge af nedetid hos outsourcing virksomheden. Dækningen omfatter driftstab i lighed med standard driftstabsdækning, men tager højde for at interne funktioner er outsourcet.

"Læs det med småt – forsikringen dækker ikke ved skader"
Cyberforsikringer er - i lighed med andre forsikringer – en kontrakt mellem forsikringstager og forsikringsgiver. Forsikringsbetingelserne indeholder dækningsklausuler, udvidelser, undtagelser og generelle betingelser. Forsikringsgiver påtager sig på grundlag af risikoinformationer at dække de omfattede tab og omkostninger, på visse betingelser. Forsikringsaftaleloven og andre love gælder i tillæg til forsikringsbetingelserne.

Medierne har beskrevet sager, hvor forsikringsgiver har afvist dækning af tab ved "CEO Fraud eller Social Engineering Fraud", hvilket i forsikringstagers optik er forkert, da forsikringen er købt for at dække "cyberkriminalitet". Det er ikke noget nyt, men vigtig at gøre det klart, at intentionen med en Cyberforsikring IKKE er at dække tab af penge ved kriminelle handlinger, som netop sker i sager om "CEO Fraud". Denne type tab dækkes af en Kriminalitetsforsikring.

Dækning under en Cyberforsikring starter når en forsikringstager oplever følgende hændelser: forstyrrelser af egne computer netværk / -systemer som følge af sikkerhedsbrist, eller en administrativ fejl eller et persondatabrud. Intentionen bag Cyberforsikring beskrives i ordlyden og definitionen af disse hændelser. Sikkerhedsbrist og cyberkriminalitet er ikke synonymer, da sikkerhedsbrist ikke nødvendigvis er en kriminel handling. Omvendt er "CEO Fraud" ikke nødvendigvis et sikkerhedsbrist.

Medierne har også fokuseret på misforståelser af undtagelser i Cyberforsikring. Undtagelser i en Cyberforsikring skal sikre, at forsikringen dækker de tiltænkte tab og omkostninger som forsikringstager oplever indenfor de risikoinformationer der ligger til grund for forsikringen. Forsikringen dækker ikke tab der udspringer af ekstraordinære begivenheder udenfor forsikringstagers / forsikringsgivers indflydelse, f.eks. krig og eksternt forsyningssvigt.

Hvordan forbedrer jeg cyber risici – og får en bedre Cyberforsikring
Virksomheder kan – afhængigt af budget – minimere og reducere cyber risici, og dermed forbedre grundlaget for tegning af Cyberforsikring. Nedenfor nogle råd og .

Generelt i relation til cyber risici:

1. Ledelsen er opmærksom på vigtigheden af IT og OT sikkerhed
2. Virksomheden har en klar strategi om at prioritere IT og OT sikkerhed og strategien implementeres iht. planer og politikker
3. CISO findes som job, med direkte reference til direktionen, hvis ikke del af direktionen (afhængigt af vigtigheden for virksomheden)
4. Tilstrækkeligt budget til at gennemføre planer
5. Cyber risici er tænkt ind i alle forretningsenheder, forsyningskæder og kontrakter
6. System og processer muliggør overblik og dokumentation
7. Alle medarbejdere trænes og testes i IT og OT sikkerhed
8. Penetrationstest, phishing and SMSishing,
9. Beredskabsplan, IT beredskabsplan, BCD, DRP, RTO, RPO m.m.
10. Forsikringspolitik

Konkret i relation til Cyberforsikring, jf EnSure cycle

A. Identificer og Forudse => hvilket tab og hvor stort?

Forsikringer sammensættes og tegnes med udgangspunkt i risikoinformation. Forsikringssum, selvrisikobeløb og præmie beregnes med afsæt i information om risici og tabsscenarier. Forsikringsselskaber kan estimere virksomheders tabsscenarier, men det er virksomheden der bedst kender risici og deraf afledte tab. Virksomheder der har analyseret forretningen og identificeret hvordan de er afhængige af IT og OT, og forsøgt at forudse hvad der sker hvis ikke IT og OT er tilgængelig har selvfølgelig en bedre forståelse for risici og dermed mulighed for at minimere og reducere risici, samt at regne på, hvad det koster hvis risici materialiserer sig. Det være sig driftstab, herunder periode og beløb inklusive meromkostninger og øgede omkostninger ved at opretholde drift. Erstatningsansvar er sværere at forudsige, da tabet beror på tredjemands tab, men man kan se på, hvilke data man er ansvarlig for; hvor meget data; hvor ligger data, hvilke geografier er involveret m.m., og gøre sig betragtninger om, hvad det koster at kompensere, monitorere, reparere samt hvor stor en bøde man risikerer at ifalde.

B. Forebyg => træning af ansatte

Ansatte er formentlig den største risikofaktor i relation til Cyber risici. Træning af ansatte er noget af det mest effektive virksomheder kan gøre for at forebygge cyber angreb . Det er alle der kan falde i og blive årsag til at et cyber angreb lykkedes. Træningen skal omfatte alle ansatte, inklusive receptionister, vikarer, studerende m.fl.. Indholdet af træningen bestemmes af virksomhedens aktiviteter, organisation og geografisk udbredelse. Træningen skal følges op af tests, både lige efter træning og et stykke tid efter. Hvis der fejles under test, må der (genop-)trænes.

IT sikkerhed er ikke kun IT afdelingens ansvar. IT afdelingen er en vigtig brik i spillet om sikkerhed, men sikkerheden er ikke bedre end det svageste led i forsvaret, og det kræver kun en utrænet, uopmærksom ansat for at et cyber angreb bliver succesfuldt for hackerne. Hvis virksomhedens ansatte føler og tager ansvar for sikkerheden er virksomheden godt rustet til at imødegå cyber risici

C. Beskyt => Segmentering

Virksomheders IT netværk og adgangen til systemer og data er essentielt for virksomheden. I tilfælde af, at netværk, systemer og data er utilgængelig, så vil de fleste virksomheder være udfordrede på at fungere.

IT nedetid resulterer for de fleste virksomheder i tab af indtjening og meromkostninger til at opretholde driften, hvorfor nedetid søgesundgået i videst mulige omfang.

Virksomheden kan minimere risici ved at segmentere netværk, systemer og data, således at der opdeles i flere sektioner, der kan åbnes og lukkes som branddøre. Jo færre adgange, des færre sikkerhedsrisici. Essentielle, forretningskritiske segmenter kan sikres ved at afskære dem helt fra Internettet og netværk, men denne tilgang giver udfordringer med at tilgå sådanne segmenter, fx for at opdatere, vedligeholde, analysere, så segmentering kan være meget kompliceret og dermed tidskrævende, hvorfor det også kræver flere ressourcer.

CYBERSECURITY BØR FÅ ØGET FOKUS

Af Nikolaj Henum.

Interview med Jesper Nytoft Bergmann.

Vi står lige nu med benene solidt plantet i den digitale tidsalder. Langt de fleste virksomheder og markeder er i fuld gang med at blive disruptede - eller også er de allerede blevet det. Og metoder og processer har ændret sig markant i samme periode på grund af ny teknologi - og vil med garanti også gøre det i årene fremover. Alt sammen takket være den teknologiske tidsalder.

Men den fantastiske teknologi og de mange medfølgende muligheder for at forbedre processer og metoder har også en lumpen følgesvend – nemlig cybercrime. En følgesvend, som man ikke skal ønske sig på besøg i sin virksomhed.

Uanset hvor meget energi og hvor mange ressourcer man bruger på cybersecurity, kan man aldrig gardere sig 100 procent imod truslerne. Flere danske virksomheder har allerede været hårdt ramt, og de økonomiske konsekvenser har i flere tilfælde vist sig enorme. Derfor har både ledelsen og bestyrelsen i en virksomhed et ansvar for at bringe dette område i spil.

»Der har været flere eksempler på store danske og også børsnoterede virksomheder, der er blevet ramt af hackerangreb. Jeg tror ikke, det er fordi, de ikke har taget cybersecurity alvorligt, men lige meget hvor mange forholdsregler, du tager, så kan du aldrig vide dig helt sikker. Den helt store udfordring i dag er jo også, at de forskellige devices i en virksomhed hænger sammen i et kolossalt netværk, og bliver du først udsat for et hackerangreb, så er der stor risiko for, at angrebet breder sig som ringe i vandet,« forklarer Jesper Nytoft Bergmann, der er Managing Director hos AVT Business School.

Han understreger, at cybersecurity allerede i dag implicit er et emne på uddannelsesinstitutionerne.

»Vi har set det i forhold hele digitaliseringsbølgen. Som executive MBA-skole har vi et stort fokus på det emne, og hele digitaliseringsdelen er i høj grad blevet integreret i undervisningen i dag. Verden er langt mere kompliceret end for bare få år siden, og det stiller ikke mindst krav til lederne. Derfor har vi også meget fokus på, at vores executive-studerende får adgang til konkrete værktøjer til at navigere i denne nye verden – og herunder til at stille de rigtige spørgsmål i forskellige kontekster, for på den baggrund at kunne træffe de rigtige beslutninger efterfølgende,« siger han.

Ansvar for bestyrelsen og omvendt

Som leder i en virksomhed skal du stå på mål for de beslutninger, som du træffer, og det ikke mindst i forhold til bestyrelsen. Og bare fordi emnet er kompliceret og svær at forstå - og måske endnu mere vanskelig at formidle – så betyder det ikke, at man må nedprioritere cybersikkerhed. Tværtimod.

»It-sikkerhed er ofte forbundet med meget specialiseret viden og vil være forbeholdt nogle få specialister, der er dygtige på den tekniske platform og måske mindre dygtige på den kommunikative del. Og det kan efterlade lederen i en svær situation, og det kan betyde, at sikkerheden bliver overset. Og på samme måde finder bestyrelsen også ofte området kompliceret - og på den måde får it-sikkerhed ofte ikke den rette bevågenhed, før hammeren er faldet, og virksomheden har været udsat for et hackerangreb,« fortæller Jesper Nytoft Bergmann.

Det betyder ikke, at ledelsen skal sætte sig ind i de finere detaljer i cybersecurity set fra et teknisk perspektiv, men en leder skal kunne foretage en risikoanalyse af virksomheden, og på samme måde, som man analyserer potentielle fremtidige konkurrenter, kursrisiko, rekruttering af nye medarbejdere med videre, skal man også afdække området inden for cybersecurity.

Og det handler ikke bare om, at man skal beskytte sig imod, at virksomhedens egne værdier bliver stjålet, for hvis virksomhedens it-systemer indeholder informationer om brugere og kunder, så skal disse også beskyttes. Dels fordi loven om GDPR kræver det, men også fordi, det kan give massive slag i virksomhedens omdømme, hvis brugeroplysninger bliver stjålet og offentliggjort.

»Det er både lederen og bestyrelsens ansvar, at it-sikkerheden ikke bliver nedprioriteret, og hvis man ikke selv er i stand til at forstå, hvorfor og hvilke risici der er forbundet hermed, så er man nødt til at inddrage specialisten og sikre, at denne også er i stand til at formidle budskabet og gøre sig forståelig over for ikke-specialister,« råder Jesper Nytoft Bergmann.

»Uden relevante og forståelige oplysninger kan du ikke vurdere din virksomheds aktiviteter i forhold
til, om du er i risikozonen for at blive udsat for et hackerangreb,« tilføjer han.

Med den hastighed som det teknologiske lokomotiv kører med for øjeblikket, har såvel leder som bestyrelse i dag fået et endnu større ansvar i forhold til at forstå og vurdere specialisten eller få denne til at gøre sig forståelig. Kun på den måde opnår man det rette grundlag i forhold til at træffe den rigtige beslutning og allokere den rette tid og ressourcer i retning af it-sikkerhed.

Board Perspectives udgives af:
Board Network, The Danish Professional
Directors Association
Grønningen 25
DK-1270 København K
CVR.nr. 34457026
ISSN: 2246-6096
Tlf. 21 28 28 82
www.boardnetwork.dk
info@boardnetwork.dk

Ansvarshavende chefredaktør:
Jakob Stengel, jsh@boardnetwork.dk

Layout
Insight Communication

Bidragsydere i dette nummer:
Global Head of Board Practice, **Jakob Stengel,**
CASE ROSE / INTERSEARCH

Senior Partner, **Gert Hemmingsen**
VALCON

CTO, **Jacob Herbst,**
DUBEX

Group Liabilities manager, **Klaus Stubkjær Andersen,**
RISKPOINT

Group Liabilities manager, **Jens Houen Zakarias,**
RISKPOINT

Director & Group CFO, **Pernille Fabricius,***P*

CEO, **Steen Buchreitz Jensen,**
SCANDINAVIAN EXECUTIVE INSTITUTE

Professor, **Stanislav Shekshnia,**
INSEAD

CEO, **Suzanne Jozefowicz**
INCORVUS LTD.

Head of PR for AVT Business School, **Nikolaj Henum**

Jakob Stengel, *cand.jur., har i 22 år beskæftiget sig med Corporate Governance samt ledelsesrådgivning, først 12 år i den finansielle sektor, og de seneste 10 år som konsulent og partner hos flere af headhunter-branchens mest fremtrædende, internationale aktører, i dag i regi af Case Rose / InterSearch (www.caserose.com), hvor han er Managing Partner og Global Head of Board Practice. Jakob er grundlægger af og formand for Board Network - The Danish Professional Directors Association, og virker tillige som bestyrelsesformand og -medlem i en række danske bestyrelser.*