Grab ‘n Go: Session 10
To have or not to have
Cyber security kompetencer
30. August 2016
#deloittegng
Chapter Zero

Who we are.
Deloitte Cyber Risk Services has an enormous global network of Security & Privacy Professionals

The Nordic practice already consists of more than 100 dedicated professionals.

Deloitte has approximately 10,000 cyber security, IT risk management, and privacy professionals globally. Many of them are certified ISO, CISA, CISSP, CISM, CEH or by SAP or Oracle.

<table>
<thead>
<tr>
<th>Region</th>
<th>Cyber security professionals</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>&gt; 4,500</td>
</tr>
<tr>
<td>EMEA</td>
<td>&gt; 1,600</td>
</tr>
<tr>
<td>Asia Pacific</td>
<td>&gt; 2,500</td>
</tr>
<tr>
<td>Rest of the World</td>
<td>&gt; 1,300</td>
</tr>
<tr>
<td>The Nordics</td>
<td>&gt; 100</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>&gt; 225</td>
</tr>
</tbody>
</table>

“Deloitte continually develops, tests, and launches methodologies that reflect a deep understanding of clients’ cyber security and help the firm stay ahead of the curve and set the bar in terms of addressing cyber security consulting needs.”* In order to stay ahead of the game, the practice puts greats emphasis on developing talent and certifying its professionals.

<table>
<thead>
<tr>
<th>Accreditation</th>
<th>Nordic cyber security practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISC2</td>
<td>Over 85 CISSP’s</td>
</tr>
<tr>
<td>EC-Council</td>
<td>Over 50 CEH’s</td>
</tr>
<tr>
<td>ISACA</td>
<td>Over 80 CISA’s, over 70 CISM’s</td>
</tr>
<tr>
<td>NOREA</td>
<td>Over 15 Registered IT Auditors</td>
</tr>
<tr>
<td>IAPP</td>
<td>10 CIPP’s</td>
</tr>
<tr>
<td>ISO</td>
<td>20 ISO-27001 Lead Auditors</td>
</tr>
</tbody>
</table>

* Source: Kennedy Consulting Research & Advisory; Cyber Security Consulting; Kennedy Consulting Research & Advisory estimates © 2013 Kennedy Information, LLC. Reproduced under license.
### Deloitte Cyber Risk Services

#### Cyber Governance Services
- Cyber strategy framework
- Cyber Threat and Risk Planning
- Cyber Business Continuity and Services Recovery Planning
- Cyber Training, Awareness and Employee Planning
- Privacy advisory service
- CISO aaaS / DPO aaaS

#### Cyber Check
- Penetration testing
- Vulnerability Management
- Threat Resiliency Analysis
- User Awareness Analysis
- Red team, Cyber Simulation and War Gaming
- Software Development Lifecycle

#### Cyber Data Protect
- Log & compliance management
- Malware and Emerging Threat monitoring
- Event correlation and incident notification
- Event hunting and Analytics
- Threat triage

#### Cyber Watch
- Brand Monitoring
- Fake Apps monitoring
- Detection of restricted corporate information outside the office
- Web fraud detection
- Cyber Threats intelligence
- Anti phishing
- Early Cyber Attack warning
- Advanced threat Intelligence
- Social Media Analytics Service

#### Cyber Monitor
- Managed Network/ Email Data Leakage Detection and Containment
- Managed Endpoint Breach Protection
- Managed Advanced Threat, Malware and Malcode Threat Management Services
- Information and Threat Resiliency

#### Cyber Incident Response
- Incident Support and Recovery
- Incident and Crisis Management
- Forensics and Advanced Threat Analysis
- Breach Respond and Recovery
- Litigation Support
- Response, Eradication, Hardening and Resiliency
Key services range from developing a cyber security strategy to security testing and managing security operations. Our service portfolio is diverse and ever adapting to our client’s needs.

<table>
<thead>
<tr>
<th>Cyber Risk Services</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cyber &amp; Privacy Advisory team</strong></td>
</tr>
<tr>
<td>Strategy &amp; Transformation</td>
</tr>
<tr>
<td>Privacy &amp; Data Protection</td>
</tr>
<tr>
<td>IAM (including eID)</td>
</tr>
<tr>
<td>Resilience &amp; Crisis Management</td>
</tr>
<tr>
<td>Cyber Risk Quantification</td>
</tr>
<tr>
<td>IT Risk Advisory</td>
</tr>
<tr>
<td><strong>Cyber Operations team</strong></td>
</tr>
<tr>
<td>Hacking</td>
</tr>
<tr>
<td>Security Operations</td>
</tr>
<tr>
<td>Cryptography Services</td>
</tr>
<tr>
<td>Covert Operations</td>
</tr>
<tr>
<td>Incident Response</td>
</tr>
<tr>
<td>Secure by Design</td>
</tr>
<tr>
<td>Product Security</td>
</tr>
<tr>
<td><strong>Cyber Subscription Services team</strong></td>
</tr>
<tr>
<td>Managed Security Services</td>
</tr>
<tr>
<td>Hacking-as-a-Service</td>
</tr>
<tr>
<td>Crypto-as-a-Service</td>
</tr>
<tr>
<td>Phishing-as-a-Service</td>
</tr>
<tr>
<td>Cyber Threat Intelligence</td>
</tr>
</tbody>
</table>
A Covert Operations team is a group of highly skilled ethical hackers that assess the security of an organization. Which is often unaware of the existence of the team or the exact assignment.

Such teams provide a more realistic picture of the security readiness than exercises, staged role playing, or pre-announced assessments.

Covert Operations teams are designed to both capture pre-agreed "flags" as well as trigger active controls and countermeasures within a given operational environment.

Through hyper connectivity and technological developments, the exposure for industrial organizations to cyber threats is growing bigger.

Cyber attacks are daily business in our continuously changing world. Companies can prepare and arm themselves through regular reporting and security scans for example. With Hacking as a Service it is possible for our clients to use all the possibilities that the Internet has to offer, while their online assets are periodically tested for vulnerabilities.
Our teams organize several big events every year

**CyberDawn**
Hackers that cripple our energy infrastructure or open our To be better prepared for such possible cyber incidents, Deloitte facilitated the first large-scale cyber exercise for the telecommunications industry in the Netherlands, called ‘CyberDawn’, where representatives from the different vital industries collaborated.

**Hacking SAP Event**
SAP is the heart of your organization which makes it vulnerable. Arm yourself against vulnerabilities and secure your system against them, by getting insight into the vulnerabilities of a SAP application and the associated infrastructure.

**Privacy with a View**
Deloitte Cyber Risk Services organizes several events around Privacy, such as privacy round tables and the annual recurring event Privacy with a View.
At Deloitte, we care: about our planet, our people and our partners.
Deloitte is a learning organization
Cyber Risk Services works in close cooperation with Deloitte Academy.

We believe it is important to share our knowledge with clients and business relations. We offer people the opportunity to participate in a training courses together with our Deloitte Cyber Risk Services professionals.

We also strongly believe that children are the future and they have to be educated about the threats and developments in the cyber landscape. Therefore we organize HackLab Highschool, a one day course in which kids will learn everything about cyber as they play.
Chapter 1
So, what’s the problem.
The attack surface is larger and easier (look in your pocket)

Attacks are exponential in frequency, complexity and outcome
Computers everywhere!

A modern car involves typical 50 computers
...and more to follow

Expected # of "Internet of Things" units
[Gartner Nov 2014]
Threats

What everybody says:
Organized Crime
Hactivism
Nation States
Terror

The real threats:
Insiders
3. Party
Competition
Bad quality
“Whoops”
Chapter II
Welcome to the dark side.
Welcome to the Dark side…

The Deep Web

The Public Web

Only 4% of Web content (~3 billion pages) is available via search engines like Google.

7.9 Zettabytes

The Deep Web

Approximately 96% of the digital universe is on Deep Web sites protected by passwords.


WHAT IF I TOLD YOU

THE DEEP WEB IS LIKE THE REAL WEB BUT WITH 90% MORE CAT PICTURES?
5 Minutters Goog’ling

Ekstrabladet.dk spredte malware
En suspekt bannerannonce på Ekstra Bladets hjemmeside har spredt virus til sitets brugere. It-chef mener at have problemet under kontrol.

Ekspert om hacket utroskabsside: Victoria Milan overlever ikke

LinkedIn formentlig hacket
Det lader til, at LinkedIn atter har problemer med sikkerheden på deres site.

Kræftens Bekæmpelse blev hacket
Kampen mod cancer blev midlertidigt erstattet af letpakkelde kvinder på Kræftens Bekæmpelser facebook-side.

El-forsyningselskab hacket: Vi aner ikke af hvem og hvordan

Anti-hackerafdeling blev selv hacket
Ups: Dansk myndigheds mainframe er på offentlig liste over usikre maskiner
En mainframe hos Moderniseringsstyrelsen har tiltrukket sig international opmærksomhed, fordi adgangen til det store jern er usikker. Læs her, hvad styrelsen gør for at lukke for hackernes adgang til mainfremen.

Terma udsat for systematisk hacking
Avancerede malware-programmer gnavede løs i fire år, inden angreb blev opdaget.

Hackers attack the energy industry with malware designed for snooping

Fremmede stater hacker sig ind i Danmarks største virksomheder
Flere spektakulære hackerangreb har de seneste år ramt dansk erhvervsliv, og også danske ministerier er under angreb. Bag står især hakere, der arbejder for den kinesiske stat, vurderer en nogle kilder.

Iran hackers targeted airlines, energy firms: report

Novozymes erkender: Vi er blevet hacket og udsat for digital spionage
Den danske enzym-virksomhed erkender, at der i flere måneder har været uønsket besøg i netværket.

Hacket dansk tømmer betalte løsepenge
Medier elsker ordet “Hacker”

Hackere kidnappede Toms firma: Ved, hvem du er
Tog data som gidsel: Betal, eller vi sletter alt, lød beskeden

Hacker kom ind via labelprinter: Tog dansk firmas it-systemer
som gidsel

Retssag mod insider-handlende hackere begynder i USA
Mindst 800 hackede pressemeddelelser er blevet brugt til insiderhandel. Sagten omfatter svindel for mere end 600 millioner kroner.

Daniel McClane | Fredag, 4. september 2015 - 15:08

It-sikkerheden sejler hos offentlige forsyningsvirksomheder
René Kornum | Offentlig it, Sikkerhed | 6. mar 07:00

Cyber-kriminelle rover dansk firma
Dansk firma offer for DDoS-afpresning

Datatyve afpresser hver femte danske firma og myndighed
Selv om antallet af hackerangreb mod private, firmaer og myndigheder stiger, så maner mej-siden til besindighed for EU-valg, der kan have strafferammen.

6 ud af 10 danske virksomheder er blevet hacket
Lidt om skoler…

Hackergruppen Anonymous truer med at hacke danske skoler.

Danske teenagere hacker sig ind på skolens IT-system - risikerer halvandet års fængsel
Tre unge mænd er mistenkt for at have hacket sig ind på et IT-system og slettet flere elevers fraværsprocenter. De risikerer ruske bag tre remer i halvandet år.
26. november 2014 kl. 12.59

Hackere saboterede test og truer afgangsprøve

13-årig lagde internet ned på skoler
Aalborg Kommune har nu sendt en reaktion på 25.000 kr. for afgang}

Elever hacker 7.000 computere for at slippe for test

Københavns Universitet lukker netværksdrev i 12 timer efter virusangreb

Sikkerhedshul p.itemView:en på 8. måned: Studerende kan snyde med karakterer

Elever havekets skolens datasystem

Datasystemet ved Gøl lidtregendende skule er hacket. Flere elever er involveret, og kan ha endet egne og andres karakterer.

Tiltale: Elever hackede skole og ændrede karakterer

Fler elever fra Københavns Tekniske Skole er tillid til for hacking, hvor ændrerne karakterer for dem selv og flere andre elever

Skoleelever fandt grumt sikkerhedshul i Københavns Kommunes software

Elever hacker afsløret i sabotage mod national test

En gruppe elever fra en skole i Hedensted, der forsøgte at sabotere den nationale test med et hackerangreb, blev afsløret, og risikerer at blive meldt til politiet.

Mann (19) hacket sød inn i skolenettet og lste rapporter om selv
Av ROGER DANIELSEN
PUBLISERT 29. oktober 2015 kl. 17:13

Skoleelever (14) hacket 33 skoler

Tenåringsskudder ville ramme sin egen skole. I stedet fikk 33 skoler i Grenland såg for hackingen.
Sundhedsdata

Kinesiske hackere mistænkt for at stjæle millioner af amerikaneres sundhedsdata

En hackergruppe, der angiveligt har bånd til den kinesiske regering, har stjålet sundhedsdata fra 4,5 millioner mennesker.

Etisk Råd: Skærp håndteringen af sundhedsdata

Vores sundhedsdata skal styres med fast hånd, men der skal ikke indsamles mindre af det, mener Etisk Råd.

Sikkerhedssjusk: 20.000 personer kan se patientdata i Region Hovedstaden

Region Hovedstadens elektroniske patientjournalsystem er ude i et ekstremt hårdt blæsevejr på grund af dårlig sikkerhed. Det ligner grov sjusk med følsomme informationer. Lyder anklagen.

Pas på dig selv, når du går til læge

Lægehushacket: Vi kan ikke komme ind på hjemmesiden

Ukendte gerningsmænd har i løbet af weekenden hacket hjemmeside tilhørende lægehus, der nu fremstår mere nøgent og vovet.

Af Jesper Markussen, jema@dagbladetholstebro.dk
Søndag den 31. januar 2016, 21:52

En nogen kvinde, der rører ved sig selv, er hvad der møder én, hvis man går ind på lægehushjemmeside.

Hacket hospital betaler 113.000 kroner til ransomware-bagmænd

Læger politianmeldt for at hacke kolleger

To jyske læger politianmeldt for at have hentet oplysninger på Medicinprofilens om 15 idrætslægers ordinationer

DAMD
Datalæk
intet nyt – bare større end før…

Advarsel: Alle danskere med en LinkedIn-profil bliver handlet på nettet

Omkring en million danskeres mailadresser og passwords bliver i disse handlet på nettet, efter et hackerangreb mod LinkedIn i 2012. Læs her, hvordan du som LinkedIn-bruger beskytter dig selv.

167 Million LinkedIn Hacked accounts on SALE!

Recently confirmed Myspace hack could be the largest yet

Posted yesterday by Sarah Perez (@sarahintampa)
## Your Product
Order safely on RealDeal.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>LinkedIn 167M</td>
</tr>
<tr>
<td><strong>Subtotal</strong></td>
<td><strong>BTC 5.0000</strong></td>
</tr>
<tr>
<td><strong>Postage</strong></td>
<td><strong>BTC 0.0000</strong></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>BTC 5.0000</strong></td>
</tr>
</tbody>
</table>

## peace_of_mind
Know your vendor.

- **Feedback of 0%**
- **Level 1**
- **Return Policy**

**Last Seen**  | **May 18, 2016**
Woops
The SONY hack

Deloitte Managers Made Huge $ Salaries, Hacked Documents Show

Deloitte & Touche LLP  SR MGR/DIR  ERS Director  LOS ANGELES  M  12/00
Deloitte Tax LLP  SR MGR/DIR  Tax Director  WASHINGTON 12TH ST  F  12/00
Deloitte Consulting LLP  SR MGR/DIR  DC Director  WASHINGTON-TYSONS  M  12/00
Deloitte & Touche USA LLP  AD EXEMPT  DIRECTOR-OPERATIONS  SPRING VALLEY-DC  M  12/00

Sony Hack Also Leaked Deloitte Salaries, Reveals Gender Gap

3 Dec 2014 / By ADRIENNE GONZALEZ

How Did 30,000 Deloitte Employees Get Caught Up in Sony’s Data Leak?
Open Source Intelligence (OSINT)

Jeres virksomheders passwords ligger også på nettet. Eksempler:

LinkedIn.com has: 6 result(s) found. Adobe database has: 1 result(s) found. Zoosk.com has: 2 result(s) found. Th

MySpace.com has: 1 result(s) found. This LinkedIn.com has: 36 result(s) found. This Adobe database has: 4 result(s) found. Th Tianya.cn (Chinese) has: 4 result(s) found. 1 7k7k.com Chinese DB has: 1 result(s) found. Renren.com (Chinese) has: 2 result(s) found. Weibo.com (Chinese) has: 1 result(s) found.

Adobe database has: 1 result(s) found.

LinkedIn.com has: 10 result(s) found. Adobe database has: 1 result(s) found. Firebug.com has: 1 result(s) found. VerticalScope Network (Vbulletin) (939 Websites) has: 1 result(s) found. Horosz2Novorth.com Part 2 has: 1 result(s) found.

LinkedIn.com has: 3 result(s) found. Adobe database has: 2 result(s) found.

MySpace.com has: 12 result(s) found. LinkedIn.com has: 177 result(s) found.

LinkedIn.com has: 3 result(s) found. Adobe database has: 2 result(s) found.
Deloitte har absolut INDET med lækkagen af data fra LinkedIn at gøre!
Deloitte benytter udelukkende åbne og frit tilgængelige kilder, til at opnå disse informationer!
Deloitte opsamler, gemmer og/eller behandler ikke disse data efter denne præsentation.
Alt bliver slettet for forsvarlig vis, og arbejdsmateriale er ikke gemt på disk.
KEEP CALM
AND
DON'T SHOOT THE MESSENGER
Hvad går man ellers efter?

- Penge, Kreditkort
- Intellectual property
- Personlige oplysninger

**Afpresning**

Derfor gik Nordea i sort i weekenden - var under heftigt hackerangreb i flere lande

Nordea var blant en af to store nordiske banker, som blev laget med i weekenden. Den fremadrede pengesagn angreb kort Swedbank og påkastede kort efter også, at man ville lave Nordea ned. Indfællet skulle få timer eller.

8 november 2013 kl. 11:13

**Hackere sælger dine oplysninger for 7 kr. på det mørke net**

Datathyveri er nu så hyppigt, at prisen på personlige data presses i bund på det sorte marked. Det samme gælder kreditkortoplysninger, viser ny rapport.

**Danish defence secrets obtained by foreign spies**

Denmark’s largest weapons company and up to four other defence targets were successfully hacked over a period of four years, and signs point to China.

**Nets spærer tusind Dankort efter hacker-angreb**

Et hackerangreb mod en butik er forklaringen på, at kortleverandøren Nets har måttet spærre godt 1.000 Dankort og kreditkort i denne uge.

30. maj 2014 kl. 11:28
### Which currency should we use?

<table>
<thead>
<tr>
<th>Service</th>
<th>Price (USD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DDos Service</td>
<td>10 (hours) or 1200 (months)</td>
</tr>
<tr>
<td>e-mail Spamming</td>
<td>10 - 150 (1,000,000 mails)</td>
</tr>
<tr>
<td>SMS Spamming</td>
<td>50-200 (100,000 sms’)</td>
</tr>
<tr>
<td>Call flooding</td>
<td>3 (hours) or 100 (week)</td>
</tr>
<tr>
<td>Botnet (full control)</td>
<td>200 (2000 bots/day - 40% online)</td>
</tr>
<tr>
<td>Fake website + deployment</td>
<td>5 - 20</td>
</tr>
<tr>
<td>Traffic redirection</td>
<td>10(US) - 60(EU) (50,000 user/day)</td>
</tr>
<tr>
<td>Dedicated Server</td>
<td>1 (basic) - 2000 (bulletproof 1Gbps)</td>
</tr>
<tr>
<td>Ransomware (winlocker)</td>
<td>10 (executable) - 100 (source code)</td>
</tr>
<tr>
<td>Trojan (Banking)</td>
<td>1,000 (executable) – 10,000 (source code)</td>
</tr>
<tr>
<td>Pay-per-Install</td>
<td>100(RU) - 250(UK) (1000 infected)</td>
</tr>
</tbody>
</table>
Hvad kan det bruges til?
"Send flere penge, Tak!
/Direktøren"
Direktør-svindel.

Danske virksomheder frarørres millioner af falske topchefer

Flere virksomheder udsættedes for "direktør-svindel"

To danske virksomheder snøret for 140 millioner gennem direktør-phishing

Flere og flere virksomheder udsættedes for 'direktør-svindel'

Stor stigning i falske emails, der lokker penge ud af virksomheder – ny sag er bare toppen af isbjerget
Hi,

Are you busy? I need you to process a wire transfer for me today. Let me know when you are free so that I can send the beneficiary's details.

Thanks

Sent from my iPhone
Selvforsvar, CEO fraud

• Awareness
• Awareness
• Awareness
• Politikker og procedurer.
• Signerede emails (Digital signatur)
Målrettede angreb
forbløffende let

Fremmede stater hacker sig ind i Danmarks største virksomheder

Flere spektakulære hackerangreb har de seneste år rumt dansk erhvervsliv, og også danske ministerier er under angreb. Bag står isere hackere, der arbejder for den kinesiske stat, vurderer en række kilder.
Online angreb

• Phishing / Spoofing
• Web-server hacking
• Netværk hacking
• Falske telefonopkald
• Brug af fundne passwords
Deloitte Phishing test

Dear colleague,

As a part of initiative to increase focus on IT security and employee awareness, we have updated company's IT policies and guidelines. You are required to read and provide your confirmation hereof, which is done by following the link below:

IT policies and guidelines 2015

Remember to confirm that you have read and understood the policies, check the top of the page.

Deadline to submit your confirmation is 11. of December 2015, we kindly ask you to respect it.

Best regards / Med venlig hilsen

IT Department
Phishing attack - eksempel

Results of the simulation are summarized on the chart:

Figur 1 Opsummering phishing mail #1
Offline angreb

- Angreb på/via Wifi. (Farlig pakke)
- USB nøgler på P-pladsen
- Falsk håndværker
- Uhyggelig gæst
- Falsk medarbejder (cloning af kort)
Chapter III

What’s my real challenge?
“Give me something audited and I’ll hack it in 5 minutes”
Time is critical – resilience is key
The difference is being able to react in minutes - not in hours and days

Day 0
Customized malware overlook your company's anti-virus solution

Day 1
Malware starts to send sensitive documents over the Internet

Day 7
Sensitive information continues to be broadcast over several days

Day 8
Security monitoring report on abnormal patterns

Day 9
Affected machines isolated and replaced, and data breach are limited

Day 2
Attack method is identified, the evidence collected and handed to the police for pursuing the hackers

Day 10
PR is familiar with instances of media coverage and intelligence shared with peers

Reputation is damaged, and heads roll
Attack patterns are changing

- Attack vectors change from technology to people
- Attack vectors are similar to normal behaviour
- More intelligent impersonal attack
- More targeted attacks
- Supply chain/partner "poisoning"
The business is concerned
Easy questions – difficult answers

CEO: “I've heard about ransomware – are we in danger?”

Board of Directors: “Are we resilient to these new cyber attacks?”

CIO: “How and how much should I invest in our cyber protection?”

Business unit: “what are the threats most relevant to my business?”
Six essential truths about Cyber Risk

1. No industry is immune
2. Cyber damage is not only financial
3. Asymmetrical attacks
4. Traditional controls are necessary, but not sufficient
5. Authorities and governments are key stakeholders with ever-increasing focus
6. Everything cannot be protected equally
General Data Protection Regulation (of personal data) – has now been approved and will be in force early 2018

**Foundation no. 1** – one continent, one law with effective penalties: Fines of up to EUR 20m or 4% of the annual global turnover.

**Foundation no. 2** – non-European companies must follow European data protection legislation, if they operate in the European market.

**Foundation no. 3** – the right to erasure data. Data authorities and the persons involved must be informed of breaches within 72 hours

**Foundation no. 4** – "one-stop-shop" for businesses and citizens.
Challenges

• Connect the dots on a wide range of topics familiarly grouped under the heading of “cyber.”

• Business executives and security professionals seldom speak the same language

• Integrating multiple competencies to create better business context and insight in the cyber strategies

• Estimation of risks and financial impact associated with cyberattacks

• Traditional approaches to calculating impacts of cyber incidents have focused largely on the direct costs

• Theft of intellectual property, the disruption of core operations, or the destruction of critical infrastructure

• Emphasize the impacts that are visible and easiest to quantify.
Truslen kommer udefra

Publicly disclosed information about data breaches only provides a partial view of how cyberattacks can impact an organization’s performance.

To take a deeper look, Deloitte analyzed the financial consequences of two hypothetical cyberattack scenarios.
Store konsekvenser

Sikkerhedsbrud

Nedetid / Operationel Stop

Bøder

Finansielle tab

Manglende overholdelse af compliance krav

Nedsat / tabte salg

Tabt tillid

Legal

Tab of IP

Omdømmeskade
The long trail of cyberattack impacts

Beyond the initial incident triage, there are impact management and business recovery stages.

These stages involve a wide range of business functions in efforts to rebuild operations, improve cybersecurity, and manage customer and third-party relationships, legal matters, investment decisions, and changes in strategic course.

Difficulty quantifying intangible factors can mask the true extent of the impact.

Intangible damages account for over 40% of the total impact.
Chapter IV

Give me the solution then!
Hvorfor den traditionelle tilgang til IT-sikkerhed er forældet
In this corner, we have firewalls, encryption, antivirus software, etc. And in this corner, we have Dave!!
Klassisk Sikkerhed

• Fokus på Hardware
• Store (dyre) Firewalls
• Stort Fokus på Antivirus
• Stort fokus på Spam-filter
• Fokus på at skifte password ofte
• Fokus på oppetid
• Alarmer og overvågning
• Specialist område
IT Sikkerhed anno 2016 = Risikostyring

• Fokus på Risiko frem for Hardware.

• Afklaret risikoappetit (af topledelsen)

• Identifikation af kritiske systemer og aktører.
  • Integritet, Tilgængelighed, Fortrolighed
  • Zone-opdeling I Risikozoner
  • Identificerede økonomiske konsekvenser

• Målbare KPI’er for sikkerhed, forståelig rapportering til ledelsen.

• Fokus på beskyttelse af kritiske komponenter – I stedet for beskyttelse af det hele.

• Erkendelse af, at medarbejderen næsten altid er den største risiko.
Overblik er nøglen
Cyber threats requires a transformation – capabilities are not enough
Three lines of defense

• **First line of defense:** Business units and the information technology (IT) function integrate cyber risk management into day-to-day decision making and operations.

• **Second line of defense:** Information and technology risk management leaders who establish governance and oversight, monitor security operations, and take action as needed, often under the direction of the chief information security officer (CISO).

• **Third line of cyber defense:** Independent review of security measures and performance by the internal audit function. For internal audit to provide a comprehensive view of cyber security, and avoid providing a false sense of security by only performing targeted audits, a broad approach should be employed.
We have grouped 29 cyber security capabilities in 4 domains:

- Governance
- Prevent
- Detect
- Respond
Cyber Security Maturity Model Comparison to other models

**ISO 27001**
- Focuses on:
  - Preventive security
  - Infosec risk assessment
  - Management commitment
- Disadvantages:
  - Controls are a checklist, what is the need for a control?
  - Gives limited guidance on APT and detect capabilities (security analytics)

**Cybersecurity Framework**
- Focuses on:
  - Critical infrastructure within United States
- Disadvantages:
  - Maturity levels are only defined at a high level

**Cybersecurity Framework**
- Focuses on:
  - Technical controls
  - Data loss prevention
  - Brand protection
  - Network & system analytics
  - User behavior analytics

**SANS 20 Critical Security Controls**
- Focuses on:
  - Technical controls
  - Policy & Standards
  - Sourcing
  - Risk Management & Compliance
  - Cyber Threat Intelligence
  - Brand Protection
- Disadvantages:
  - Not an open model

**Deloitte**
- Focuses on:
  - FSI content pack
  - Detailed maturity guidance
  - Scope encompasses at ISO 27001, NIST and SANS controls
- Advantages:
  - Uses existing open standards like ISO 27001 and NIST and combines it with Deloitte expertise worldwide
  - Has been validated by security professionals worldwide
  - Clients use the Deloitte model for their operational internal control system
- Disadvantages:
  - Updated each Quarter with the latest industry experience
Understand the business, know your business risk – and risk appetite
Deloitte’s Cyber Capability Framework
Allowing intelligent decision taking for managing cyber resilience

**Stakeholders (Internal & External)**

**Executive dashboard for managing Cyber Resilience across the organisation**

**Cyber Threat Model**
- **Threats**
  - Gather Information
  - External system attack
  - Gain Physical Access
  - Targeted malware against workforce
  - ...
- **Scenarios**
- **Threat Actors**
  - Competition
  - Criminals
  - Customer
  - Hackers
  - Insiders
  - ...

**Business Services**
- **Organisational structure**
  - BU1
    - Business service 1
    - Business service 2
    - Business service 3
  - BU2
    - Business service 1
    - Business service 2
    - Business service 4
  - BU3
    - Business service 1
    - Business service 2
    - Business service 3
  - BU4
    - Business service 1
    - Business service 2
    - Business service 3

**Communication channels & characteristics**
… against various cyber threats ….

Not all cyber threats are equally threatening your business

<table>
<thead>
<tr>
<th>Threat Actors</th>
<th>Motives</th>
<th>Targeted Assets</th>
<th>Possible Impacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Competition</td>
<td>Making a statement</td>
<td>- Financial Data</td>
<td>• Financial loss</td>
</tr>
<tr>
<td>Criminals</td>
<td>Gain competitive advantage</td>
<td>- Intellectual Property</td>
<td>• Reputation harm</td>
</tr>
<tr>
<td>Customers</td>
<td>Espionage</td>
<td>- Sensitive Operational Information</td>
<td>• Lawsuit</td>
</tr>
<tr>
<td>Hackers</td>
<td>Disruption</td>
<td>- Services</td>
<td>• Regulatory sanctions</td>
</tr>
<tr>
<td>Insiders</td>
<td>Financial Gain</td>
<td>- Brand image</td>
<td>• Loss of trust</td>
</tr>
<tr>
<td>Organized Crime</td>
<td></td>
<td></td>
<td>• Continuity of service</td>
</tr>
<tr>
<td>Press</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protest Groups</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>State Agencies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Terrorists</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
... against various cyber threats ....
Not all cyber threats are equally threatening your business

The Deloitte Cyber Threat Model: includes 12 cyber threats, based on CAPEC’s Mechanisms of Attack.

In the threat view (right), these Deloitte cyber threats are mapped according to three dimensions:

• Does the organisation focus on preventing the risk or detecting and responding to it if it occurs?

• Is the risk known and understood (does it relate to a current threat), or unknown with little or no understanding (a future threat)?

• How resilient is our organisation to these threats and does this differ across the business?
In order to define your Cyber Threat Landscape, you need to understand the characteristics of your Business Services and related communication channels:

- Who is using the Business Service?
- Which information is accessible through the Business Service?
- Which connectivity is available (Internet, Managed IP, internal network)?
- Which technology is used?

## Organisational structure

<table>
<thead>
<tr>
<th>BU1</th>
<th>BU2</th>
<th>BU3</th>
<th>BU4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business service 1</td>
<td>Business service 1</td>
<td>Business service 1</td>
<td>Business service 1</td>
</tr>
<tr>
<td>Business service 2</td>
<td>Business service 2</td>
<td>Business service 2</td>
<td>Business service 2</td>
</tr>
<tr>
<td>Business service 3</td>
<td>Business service 3</td>
<td>Business service 3</td>
<td>Business service 3</td>
</tr>
</tbody>
</table>

## Communication channels & characteristics

Include your organisational structure, geographical locations, criticality of the business, etc. This organisational structure represents what you want to protect against cyber threats.
In the beginning there was the traditional information security headed by the CISO

Then, there is new governance required involving executives to understand and manage cyber risks

Today, cyber threats require new cyber capabilities in order to mitigate cyber risks
In the beginning there was the traditional information security headed by the CISO.

Then, there is new governance required involving executives to understand and manage cyber risks.

Today, cyber threats require new cyber capabilities in order to mitigate cyber risks.

... focussing on the right cyber capabilities
Building what you need, not what other companies do ...
... focussing on the right cyber capabilities
Building what you need, not what other companies do …

**In the beginning** there was the traditional information security headed by the CISO

**Then**, there is new governance required involving executives to understand and manage cyber risks

**Today**, cyber threats require new cyber capabilities in order to mitigate cyber risks
In the beginning there was the traditional information security headed by the CISO.

Then, there is new governance required involving executives to understand and manage cyber risks.

Today, cyber threats require new cyber capabilities in order to mitigate cyber risks.

... focussing on the right cyber capabilities
Building what you need, not what other companies do ...
Easily identify those areas which need improvement

Level of cyber resilience can be compared across the organisation (e.g. business unit, entity or service)

Select a specific cyber threat and identify how resilient the different parts of the organization are
Vertical axis shows whether a cyber threat requires focus on detective or preventive controls given the current state of technology.

Overview of the different cyber threats and the current level of cyber resilience of a specific part of the organization.

Horizontal axis shows how well a specific threat is currently understood.
Eksempel på hvordan vi skaber overblik hos vores kunder.
Udvikling fra reaktiv til proaktiv Risk Management

Gaps i traditionelle Risk Management Systemer
Deloittes Managed SIEM løsning

Deloittes synergi mellem teknologi, processer og professionelle Cyber security kompetencer

I alle aspekter af Deloittes Managed SIEM løsning samt infrastrukturen i Deloittes CyberSOC, er de højeste sikkerhedsstandarder taget i betragtning, kombineret med oplevelsen af supportteamets levering af Managed Security Services.
Identificering af eksterne krav til logning, fx
- Persondatalov / Persondataforordningen
- Sikkerheds-bekendtgørelsen
- Direktiv om net- og informations-sikkerhed, NIS
- Etc.

Risikoprofil
- Identificering af trusselbillede
- Identificering af kritisk data, personfølsom som data og kritiske systemer
- Identificering af modenhedsniveau for it sikkerhed

SIEM governance struktur
- Roller & ansvarsbeskrivelse herunder eskalationsproces
- Proces for security incident håndtering, herunder kategorier og ratering
- Udarbejdelse af Use Cases

Identificering af Risikoprofil
Security Intelligence review

Indsamling rå logs
Indsamling af rå logs

Endpoint Detection & Monitoring
- Servers, AV
- Endpoint, AV
- Web
- Client

Network Detection & Monitoring (NDM)
- Firewall
- IDS & IPS
- Web Filters
- Netflow

Identity & Data Monitoring (NDM)
- DNS and DHCP
- Database
- Active Directory
- Asset & Configuration Management Systems

Data-korrelation
Normalisering af logs

Vulnerability Data, Patch level
Asset Data
Threat Data
Konfigurations parametre

Data-berigelse
Identificering af offenses

IBM X-Force
Honeypots
Deloittes scanings resultater

Security intelligence analyse
Analysering af offenses

Kognitiv analyse
Metodisk analyse
Cyber trusselbillede

Værdiskabende kunde indsigt
IRT, Incident Response team
Månedlig Data Breach rapport med afsæt i kundens risikoanalyse
Løbende validering af kundens modenhedsniveau
And finally ... Stop talking about security

Board of Directors: "What is our risk by establishing us in UK?"

CEO: “Can we be hit by ransomware?”

CISO: “Tell me the critical success factors, then I put them in relation to our threat and current protection – and then we can discuss how it matches your appetite.”

CISO: "Yes. But we detect it and react quickly, so it will have no impact.”
Afslutning
Tak for i dag!