Nyt fra USA - Cybererklæringer

Sikkerhed og Revision 2017

v/ Per Højmark

Building a better working world

EQUIFAX

Equifax Announces Cybersecurity Incident Involving Consumer Information

Sep 07, 2017

No Evidence of Unauthorized Access to Core Consumer or Commercial Credit Reporting Databases

Company to Offer Free Identity Theft Protection and Credit File Monitoring to All U.S. Consumers

ATLANTA, Sept. 7, 2017 /PRNewswire/ -- Equifax Inc. (NYSE: EFX) today announced a cybersecurity incident potentially impacting approximately 143 million U.S. consumers. Criminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017. The company has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases.

The information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed. As part of its investigation of this application vulnerability, Equifax also identified unauthorized access to limited personal information for certain UK and Canadian residents. Equifax will work with UK and Canadian regulators to determine appropriate next steps. The company has found no evidence that personal information of consumers in any other country has been impacted.

EY

Agenda

- AICPA – hvad er ”SOC for Cybersecurity”
- Hvorfor ”SOC for Cybersecurity”
- Indhold og omfang
- Betydning

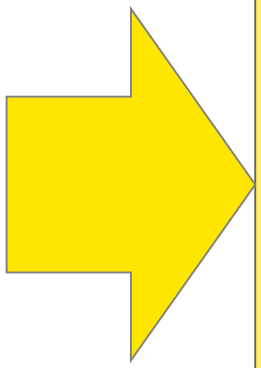
AICPA – hvad er SOC for Cybersecurity

- AICPA har i mange år været involveret i revision af it kontroller
  - 1992: SAS 70
  - 1997: Web Trust
  - 2003: Trust Service Principles and Criteria
  - 2010: SSAE 16
  - 2011: SOC1, SOC2 og SOC3
  - 2017: SSAE 18

- 1. maj 2017: “Guide – Reporting on an Entity’s Cybersecurity Risk Management Program and Controls” - SOC for Cybersecurity

Hvorfor SOC for Cybersecurity ?
- baggrund

- Trusler og udfordringer omkring cybersikkerhed er voksende
- Stigende anvendelse af og interaktion med eksterne parter
- Interessenter (interne og eksterne) efterspørger tillid til virksomheder og organisationers cybersikkerhed
- Stigende sektor fokus på håndtering af cybersikkerhed
- Mange decentrale spillere med del løsninger



Behov for en ensartet og transparent rapportering om en virksomheds / organisations risikostyrings program på cybersecurity området

SOC for Cybersecurity
- mål

- Målet for ”SOC for Cybersecurity” er en standard til vurdering af risikostyringsprogram for cybersikkerhed på virksomhedsniveau, ikke systemniveau.

- **Mere relevant information** om effektiviteten af en virksomheds / organisations risikostyrings program
- **Mere sikkerhed** for integriteten af de oplysninger, der leveres
- **Mere klarhed** omkring risikostyrings-programmets styrke til at forebygge, opdage og håndtere et betydeligt cybersikkerheds brud

Gennemsigtighed

Integritet

Pålidelighed

SOC for Cybersecurity
--basis

- For at kunne efterleve målene for ”SOC for Cybersecurity” har AICPA defineret en række delområder, som rapporteringsværktøj skal efterleve:
  - Fælles kriterier for **information** om en virksomheds risikostyringsprogram
  - Fælles kriterier for **vurdering** af programmets effektivitet
  - Give nødvendig information til interessenter
  - Flexibelt
  - Frivilligt
  - Ensartet/sammenlignelighed

SOC for Cybersecurity
- indhold og omfang

- Rapportering efter ”SOC for Cybersecurity” omfatter 3 komponenter:
  - 1. Ledelsens beskrivelse af virksomhedens/organisationens risikostyringsprogram vedrørende cybersikkerhed
  - 2. Ledelsens udtalelse om beskrivelsen af risikostyringsprogrammet og om at kontroller har fungeret effektivt for at opnå virksomhedens mål for risikostyringen
  - 3. Revisors erklæring om ledelsens beskrivelse og effektiviteten af kontrolelementer til at opfylde virksomhedens / organisationens mål for risikostyringen.

SOC for Cybersecurity
- ledelsens beskrivelse af sit risikostyringsprogram

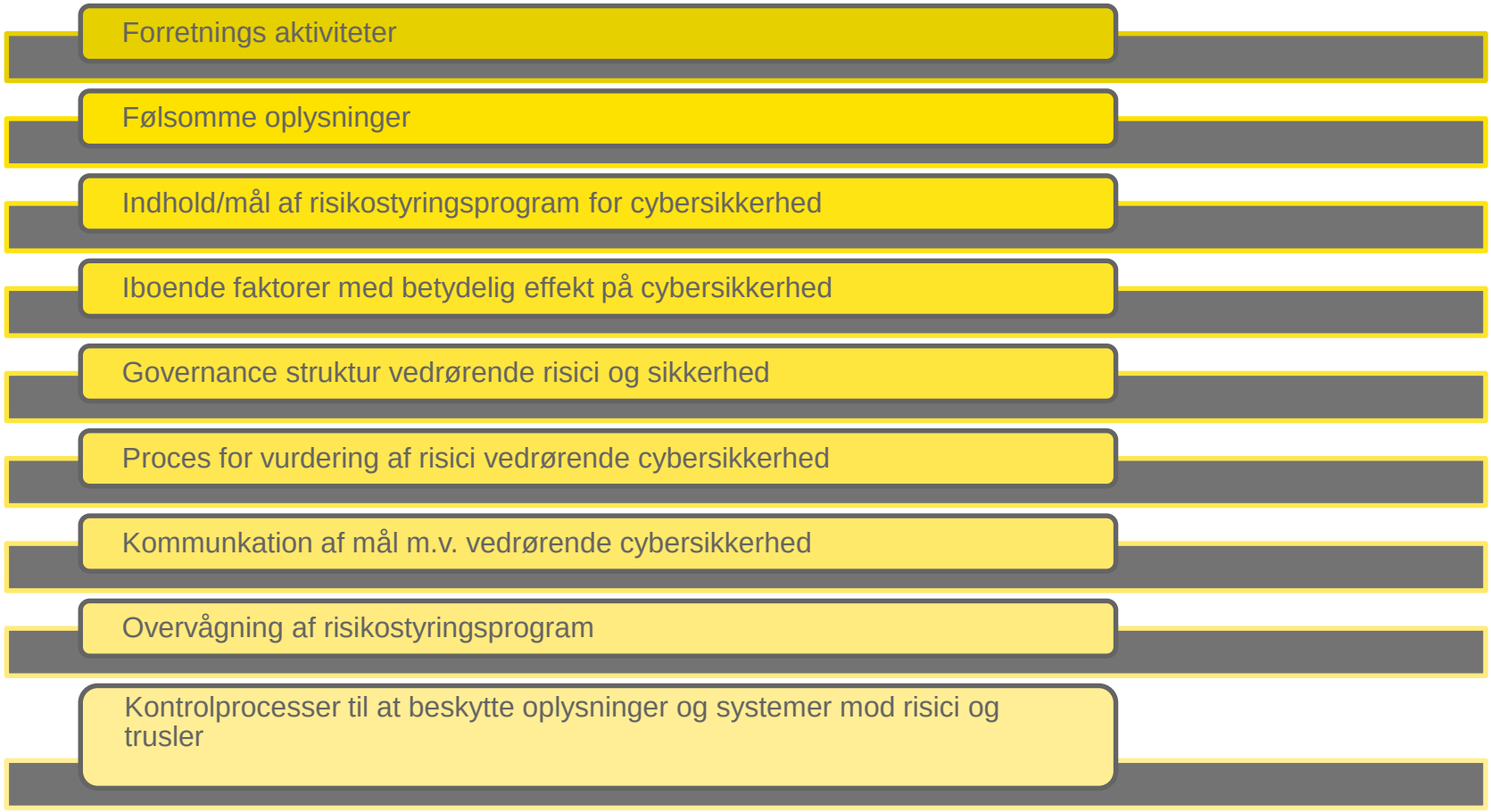
- Et risikostyringsprogram er politikker, processer og kontroller, som er designet til at beskytte information og systemer fra sikkerhedshændelser, og at opdage, reagere på og afbøde sikkerhedshændelser, samt evt. genoprette systemer og informationer.

- "SOC for Cybersecurity" indeholder 19 beskrivelseskriterier indenfor 9 områder som skal indgå i ledelsens beskrivelse

- AICPA har suppleret de 19 beskrivelseskriterier med implementeringsguider, som nærmere specificerer forhold til indholdet af ledelsens beskrivelse – i alt mere end 100 specifikke forhold, som bør overvejes af ledelsen

SOC for Cybersecurity
- ledelsens beskrivelse af risikostyringsprogram

- De 9 områder omfatter:



SOC for Cybersecurity
- revisors erklæring

- I SOC for Cybersecurity skal revisor erklære sig om ledelsens beskrivelse og effektiviteten af kontroller, dvs:
  - Om beskrivelsen af virksomhedens risikostyringsprogram for cybersikkerhed præsenteres i overensstemmelse med beskrivelseskriterierne og
  - Om kontrollerne i risikostyringsprogrammet er baseret på de fastsatte kontrolkriterier og har været effektive til at nå virksomhedens mål for cybersikkerhed.
- Revisors erklæring giver ikke sikkerhed for at virksomheden/organisationen ikke kan blive ramt af et sikkerhedsnedbrud m.v.

SOC for Cybersecurity
- kontrol kriterier og revisors erklæring

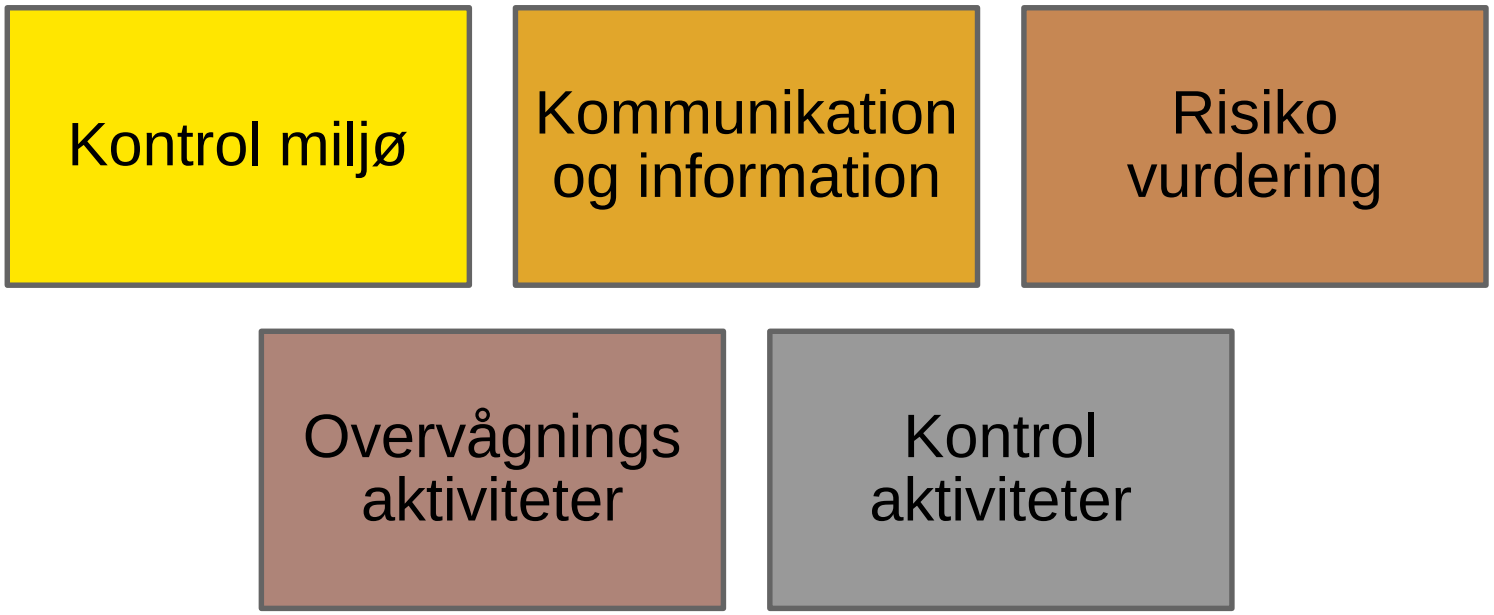
- Det er ledelsen der vælger kontrolkriterier for vurdering af ledelsens beskrivelse.
- Revisor skal vurdere om de valgte kontrolkriterier er passende.

- Kontrolkriteriern i “SOC for Cybersecurity” til brug ved vurdering af ledelsens beskrivelse er baseret på AICPA’s Trust Service Principles sec. 100.

- I AICPA’ s “SOC for Cybersecurity” er kontrolkriterierne afgrænset til:
  - Security
  - Availability
  - Confidentiality

SOC for Cybersecurity
- kontrol kriterier og revisors erklæring

- Trust Services Criteria og fokuspunkter gældende for cybersecurity omfatter mere end 200 målepunkter indenfor følgende hovedområder:



SOC for Cybersecurity
- - betydning

- Er der plads til/behov for ”SOC for Cybersecurity” ?

- På sigt - ja – fordi:

  - Interessenter (eksterne/interne) vil have tillid
  - Lovkrav/regulatoriske krav
  - Udfordringen forsvinder ikke

EY | Assurance | Tax | Transactions | Advisory

Om EY
EY er en af verdens førende organisationer inden for revision, skat, transaktioner og rådgivning. Den indsigt og de ydelser, vi leverer, hjælper med at opbygge tillid til kapitalmarkederne og den globale økonomi. Vi udvikler dygtige ledere og medarbejdere, som sammen leverer det, vi lover vores interessenter og bidrager til, at arbejdsverdenen og arbejdslivet fungerer bedre - for vores medarbejdere, vores kunder og det omgivende samfund.

EY henviser til den globale organisation og kan referere til et eller flere medlemsfirmaer inden for Ernst & Young Global Limited, som hver især udgør en selvstændig juridisk enhed. Ernst & Young Global Limited, som er et engelsk 'company limited by guarantee', yder ikke kunderådgivning. Flere oplysninger om vores organisation kan findes på ey.com

Dette materiale er udarbejdet alene til orientering, og oplysningerne i det tilsigter ikke at være fyldestgørende, og de træder ikke i stedet for udførlige analyser eller udøvelsen af professionelle skøn. I konkrete sager opfordres brugere til at henvende sig til EY's rådgivere.

ey.com/dk