

# Cyber Security and the BoD

Styreinstituttet 11. januar 2019

André Årnes

telenor group

## Connecting you to what matters most Empowering societies.

## Cyber security attacks seriously affect the reputation, trust and operations of targeted businesses

WannaCry Ransomware re-emerges at Boeing Forbes, March20<sup>h</sup> 2018



28th of March Boeing commercial airplane factory in South Carolina was hit by the WannaCry virus.

The Wanancry ransomware infected millions of Windows systems in around150 countries.

Swisscom data breach exposes 800,000 customers, Reuters, Feb 7th 2018

3

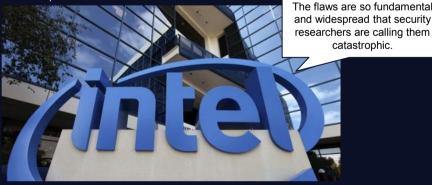


misappropriated the access rights of a sales partner, gaining unauthorized access to customer data.

50 million Facebook profiles harvested for Cambridge Analytica in major data breach The Guardian. March 17th 2018



Apple says Spectre and Meltdown vulnerabilities affect all Mac and iOS devices, BBC, Jan 4th 2018



Data of 143 million Americans exposed in hack of credit reporting agency Equifax, Washington Post, Sep 5th 2017



After the company disclosed the hack. Equifax shares plummeted 12 percent in after-hours trading.

Equifax is facing a demand to disclose the full extent of last vear's data breach. following a report that it was bigger than previously disclosed.

Deloitte hit by cyber-attack revealing clients' secret emails

Guardian, Sep 25th 2017 YOU HRVE HACKED

The hacker compromised the firm's global email unrestricted "access to all areas".



The breach affected up to 350 clients, some of which were very high profile, including US government departments.

### The expectations to security continue to increase

Changing threat landscape

New technological risks and geopolitical instability Cyber domain increasingly legislated

hanging legal

landscape

Increased expectations

Increased awareness leads to increased reputational risk

### In order to understand cybersecurity we need a solid understanding of threat actors and their motivation



## The role of the BoD in Cybersecurity

#### **Challenges for the BoD**

- Security is en **enterprise issue** affecting all parts of the organization. It is not «just IT».
- Risks, threats and vulnerabilities are often underreported and not understood.
- The issues are complex and requires expert competencies.
- Security is sensitive to **conflicts of interest** and segregation of duties is required.
- **BoD members are regularly targeted** by cyber attacks (e.g., phishing, fraud).

#### **BoD responsibilities**

- Security is a BoD level issue, a fidiciary duty representing a top enterprise risk that is hard to quantify.
- Stricter regulations and consequences increase the BoD responsibility.
- **BoD responsibilities** include setting expectations, monitoring the risks and sufficiency of governance (e.g., frameworks), capabilities (e.g., competancy) and plans.
- The **BoD needs to have competency** to understand and challenge management.
- Structured monitoring at BoD and committee level needs to be secured.

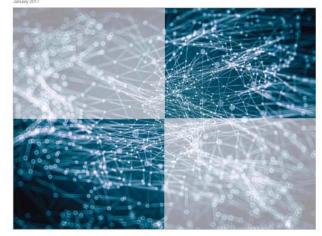
# Cyber security toolkit for BoD members and Top management

COMMITTED TO IMPROVING THE STATE

Future of Digital Economy and Society System Initiative

#### Advancing Cyber Resilience Principles and Tools for Boards

In collaboration with The Boston Consulting Group and Hewlett Packard Enterprise





THE DEFINITIVE CYBERSECURITY GUIDE FOR DIRECTORS AND OFFICERS

Georgia Institutes for Information



