




# Cyber Security and the BoD

Styreinstituttet 11. januar 2019

André Årnes



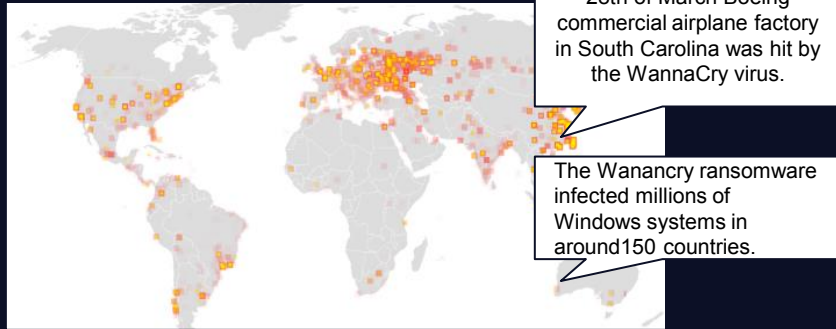
Connecting you to what matters most.  
Empowering societies.





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

**WannaCry Ransomware re-emerges at Boeing**  
Forbes, March 20<sup>th</sup> 2018



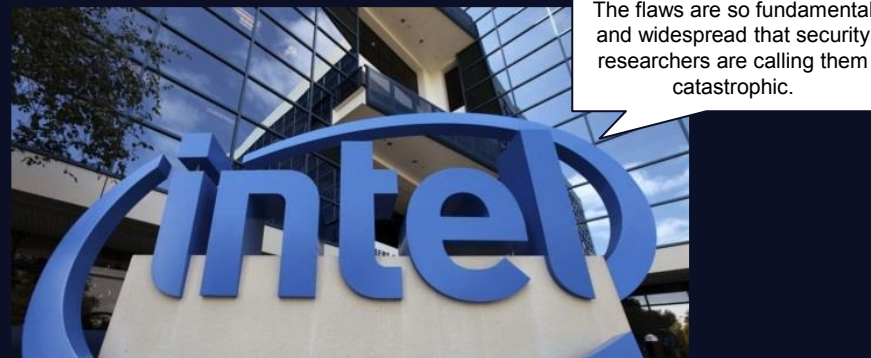
**Swisscom data breach exposes 800,000 customers**, Reuters, Feb 7<sup>th</sup> 2018



**50 million Facebook profiles harvested for Cambridge Analytica in major data breach**  
The Guardian, March 17<sup>th</sup> 2018



**Apple says Spectre and Meltdown vulnerabilities affect all Mac and iOS devices**, BBC, Jan 4<sup>th</sup> 2018



**Data of 143 million Americans exposed in hack of credit reporting agency Equifax**, Washington Post, Sep 5<sup>th</sup> 2017



**Deloitte hit by cyber-attack revealing clients' secret emails**  
Guardian, Sep 25<sup>th</sup> 2017



# The expectations to security continue to increase



New technological  
risks and geopolitical  
instability

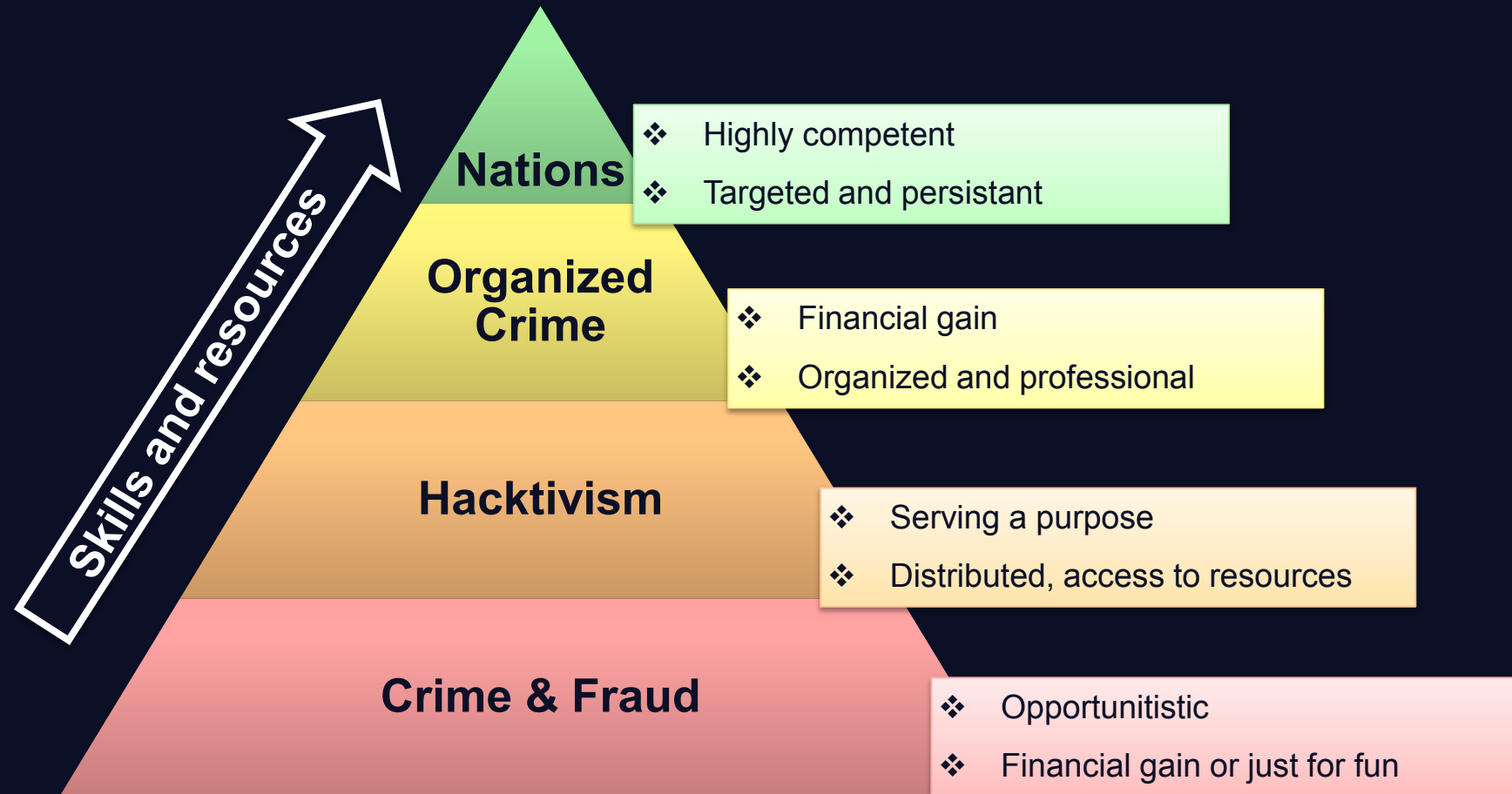


Cyber domain  
increasingly legislated



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 an **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 fiduciary 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., competency) 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

