orange™

Cyberdefense

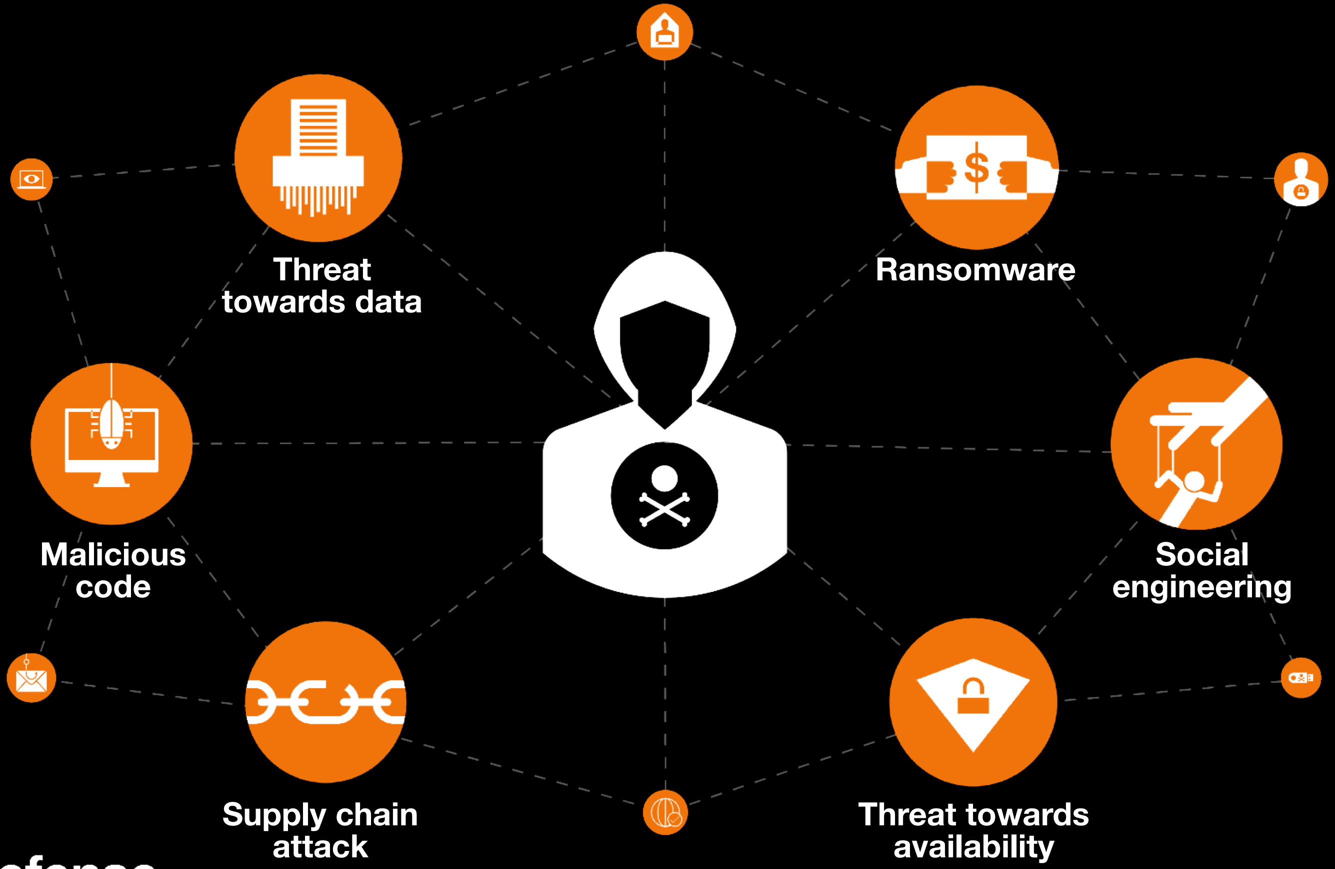
Orange
Cyberdefense

GRC

- International Presence & Skills
- Strong in the Nordics
  - Very close cooperation between Denmark, Sweden and Norway

Resilience?

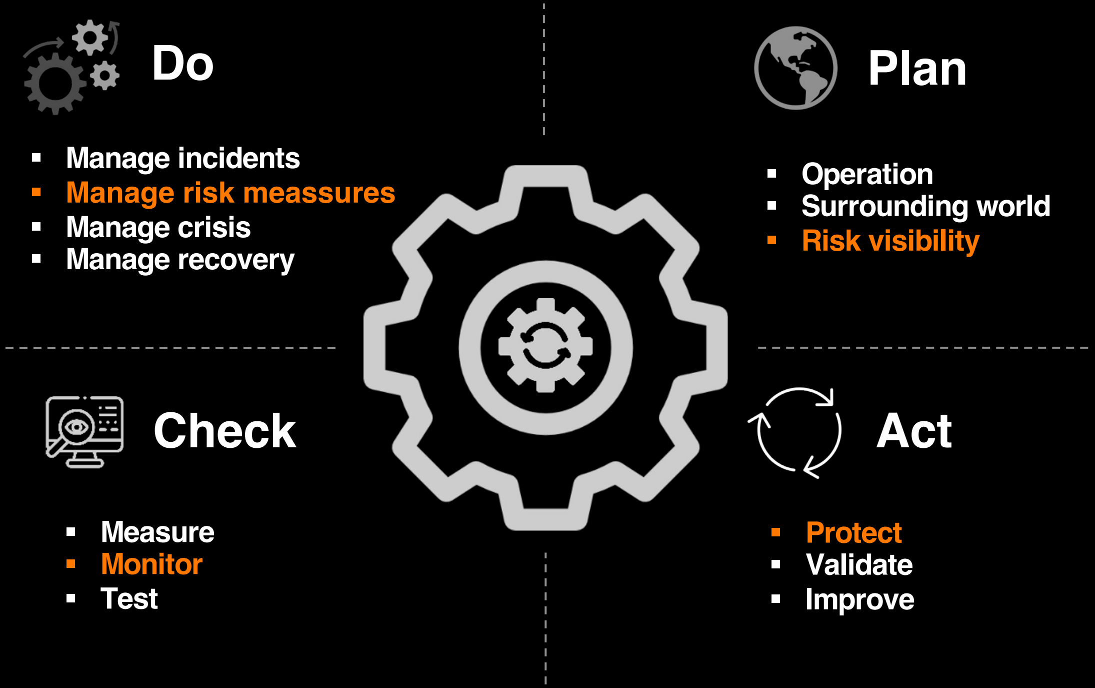
Threat Landscape.



orange™ Cyberdefense

GRC.

Risk based systematic security approach



Do

- Manage incidents
- Manage risk meassures
- Manage crisis
- Manage recovery

Plan

- Operation
- Surrounding world
- Risk visibility

Check

- Measure
- Monitor
- Test

Act

- Protect
- Validate
- Improve

…ensuring increased business resilience is now a board-level matter, too.

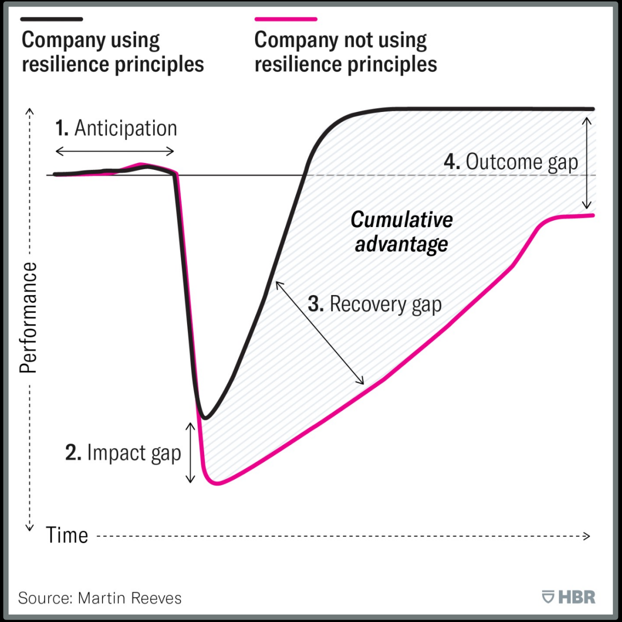
The benefits of resilience

Anticipate threats faster

Better resistance to the initial shock

Rebound more quickly

Benefit from increased fitness post shock

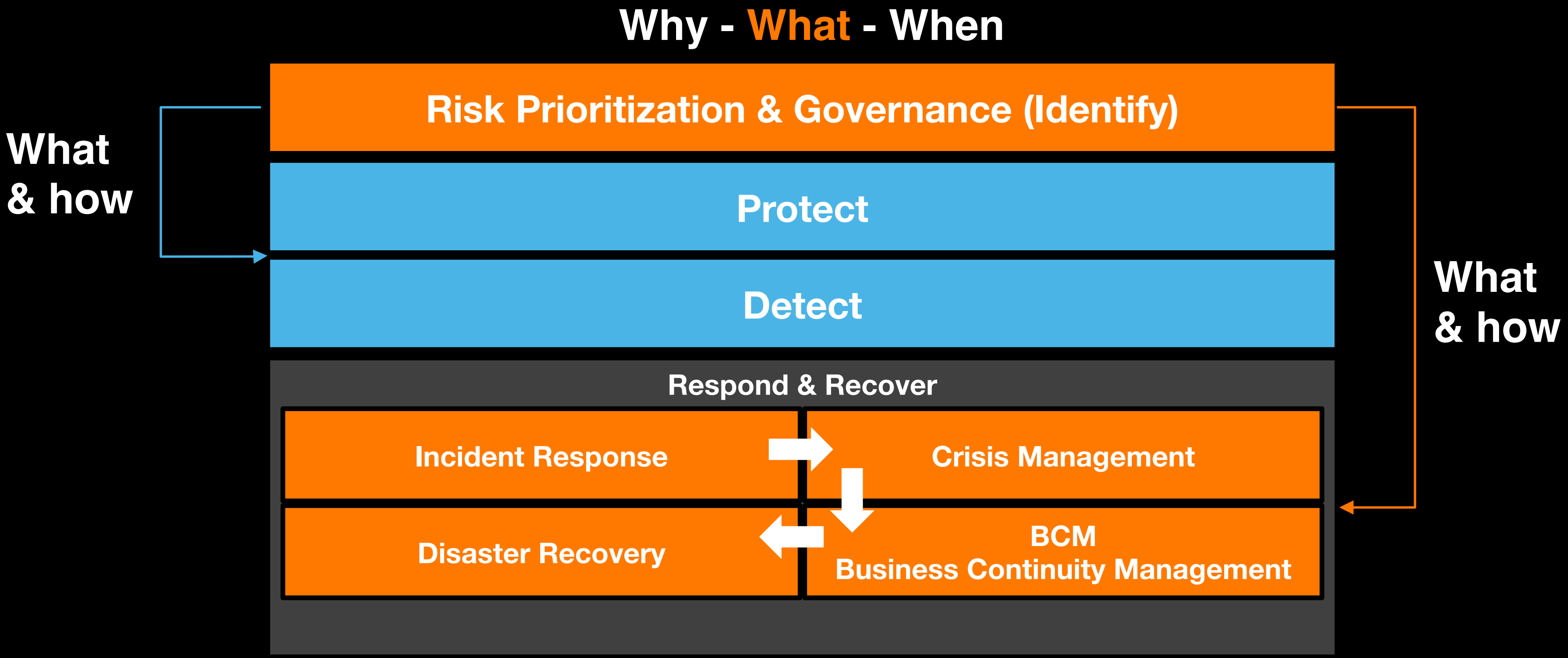


Source: Martin Reeves

Source: A Guide to Building a More Resilient Business, Harvard Business Review.

GRC - optimizing and operationalizing risk mitigation & investments

Significant part of organizational resilience



Our recommended approach will ensure seamless resilience within the required timeline.

This enables You to…

… build a security resilience plan with embedded visibility & threat intelligence

… bridge your security gaps and focus on running your business efficiently.

… ensure business continuity, even in case of disruption.

… be prepared for security conformity assessments and take care of them with serenity & peace of mind.

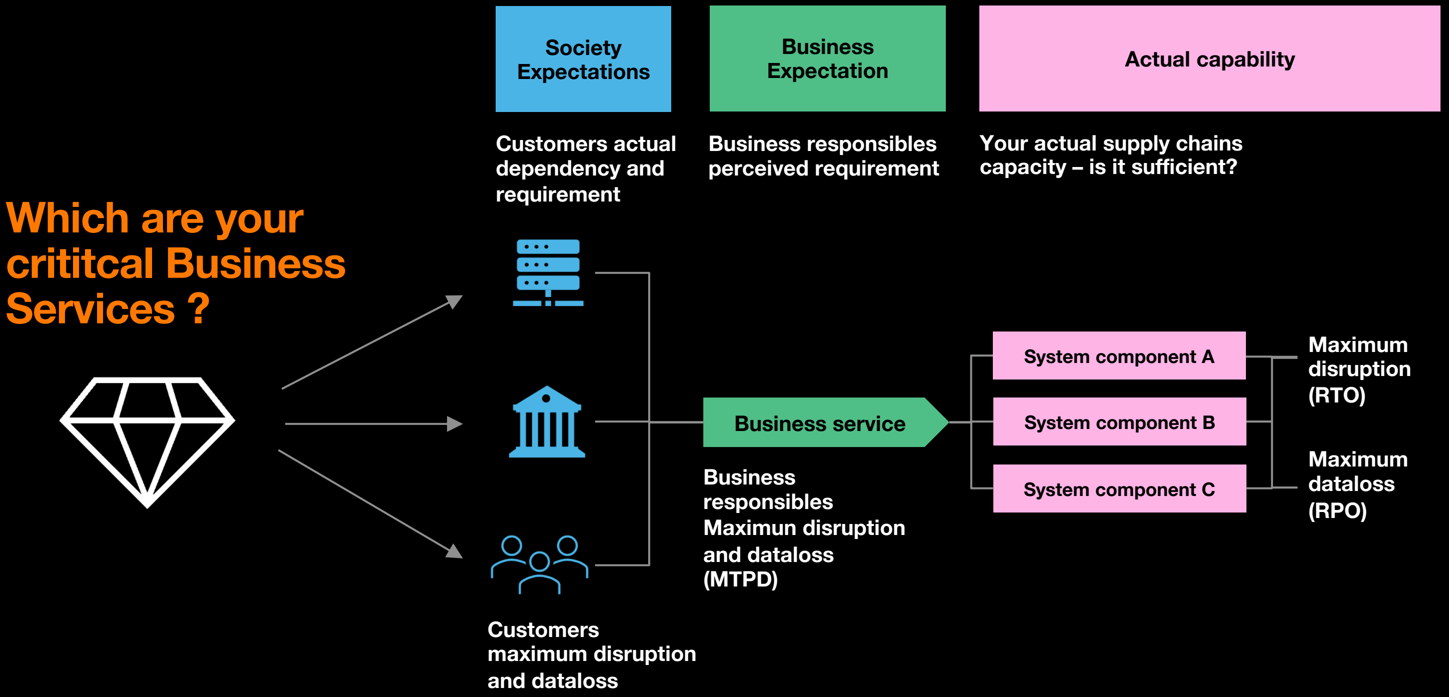
GRC Needs & Challenges

- Are our (critical) business risks adressed sufficiently?
- Are security policies interpreted and operationalised correctly?
- Visibility of who and what has accesss to what?
- Visibility of what is implemented and if it is done correctly?
- Do I have enough ressources for timely implementation?
- Are we sufficiently efficient on detecting and blocking attacks in a timely fashion?

Transparent prioritization, reporting and execution based upon business risk!

Risk Prioritisation & Governance

Which business functions are most critical?



Which are your crititcal Business Services ?

Society Expectations

Customers actual dependency and requirement

Business Expectation

Business responsibles perceived requirement

Actual capability

Your actual supply chains capacity – is it sufficient?

Customers maximum disruption and dataloss

Business service

Business responsibles Maximun disruption and dataloss (MTPD)

System component A

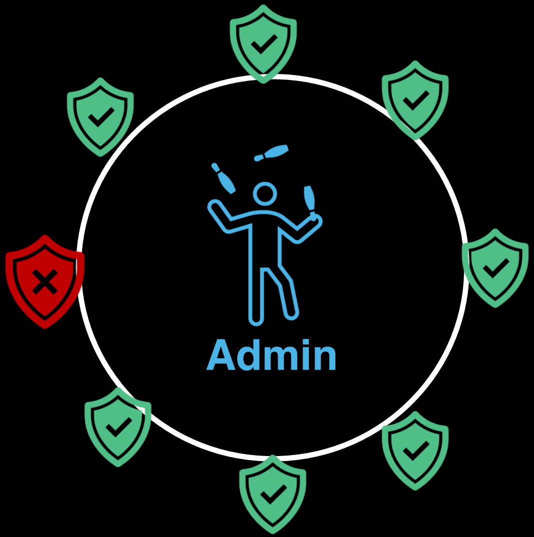
System component B

System component C

Maximum disruption (RTO)

Maximum dataloss (RPO)

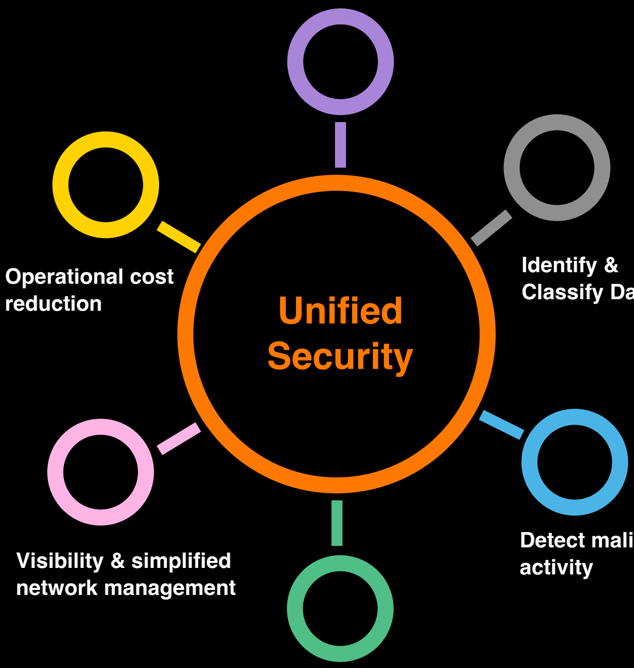
Reality Of Business Today!



- Employees work everywhere
- Employess work across many devices and solutions
- Increasing cooperation across organisations and individuals
- Cooperation across solutions and devices

Is it efficient and sufficient that security administration is performed separately in each component?

Changing The Game – SASE a modern approach



Authenticate Users and Devices

Identify & Classify Data

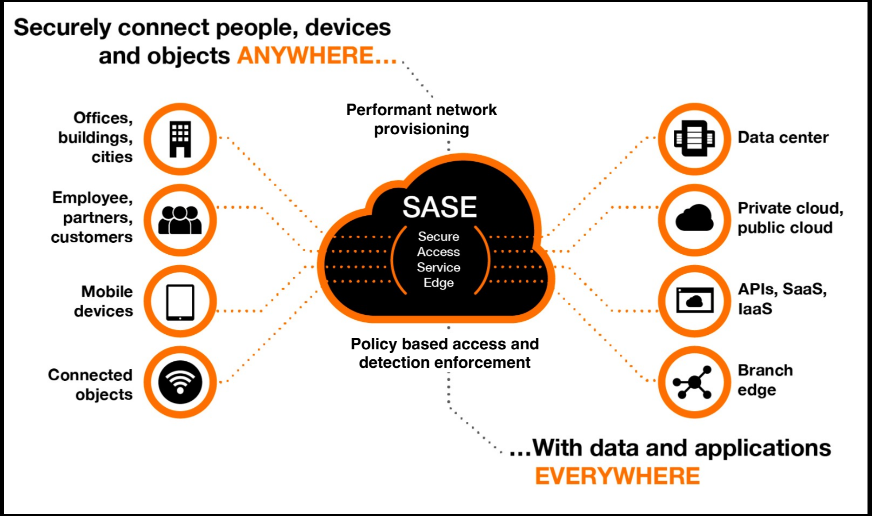
Detect malicious activity

Consistent cloud protection

Visibility & simplified network management

Operational cost reduction

Unified Security



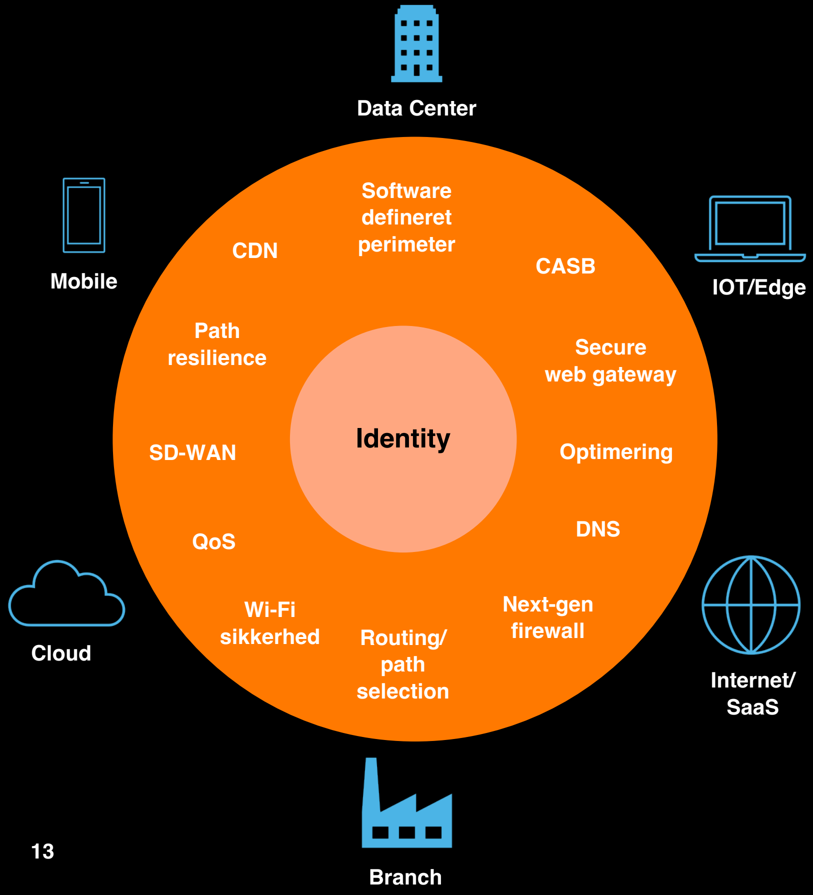
Securely connect people, devices and objects ANYWHERE…

Offices, buildings, cities
Employee, partners, customers
Mobile devices
Connected objects
Performant network provisioning
SASE
Secure Access Service Edge
Policy based access and detection enforcement
Data center
Private cloud, public cloud
APIs, SaaS, IaaS
Branch edge

…With data and applications EVERYWHERE

Business driven central control and visibility!

Changing The Game - SASE a modern approach



- **Business driven security policies sets the scene**
  - Business driven risk management defines acccess
- **Taking offsett in identity visibility**
  - Individuals, Devices, Solutions
- **Dynamic access control based upon**
  - Type, Status, Verification, Location, Criticality, etc.

Real world example

Strengthening of operational capability: Prioritization, Protection and Recovery

- Technically mature customer
- Performed Top-Down BIA
- Production and distribution of most importance
- 90% of production & distribution depended on it-infrastructure

→ 4 months later they had trained and could document recovery of IT-infrastructure within 24 hours

Cyberdefense

Success factors

1. Systematic prioritized security enables secure digitalization and continuity in digital services

2. Increases actual security level

3. Change takes time - take it stepwise

4. Don’t get lost in details

5. The Business needs to be involved and part of the journey
   - Before change is initiated
   - Business needs must be the driver (setting the frame)

Resilience anticipation – learnings matter!

Tacoma Bridge

GRC

Bo Drejer, GRC Manager
bo.drejer@orangecyberdefense.com
+45 2148 0381

orange™ Cyberdefense

Copenhagen Live 2024

orange™

Cyberdefense

Building a safer digital society.