Norwegian Maritime Cyber Resilience Centre

Our Vision:
Unified resilience against cyber threats for Norwegian Shipping and Maritime Sector

NORMA CYBER

Our Values:
Trusted
Solid
Innovative

Our Set-Up:
Mutually owned by Norwegian Shipowners and Operators

DEN NORSKE KRIGSFORSIKRING FOR SKIB
GJENSIDIG FORENING
The Norwegian Shipowners' Mutual War Risks Insurance Association

Norges Rederiforbund
Norwegian Shipowners' Association

Current Overview

110 Member organisations

Represented with 2 257 Vessels

12 Employees

Offices and Operations Room in Oslo, Norway

Services:

- Intelligence & information sharing

- Response

- Security Operations

Our members:

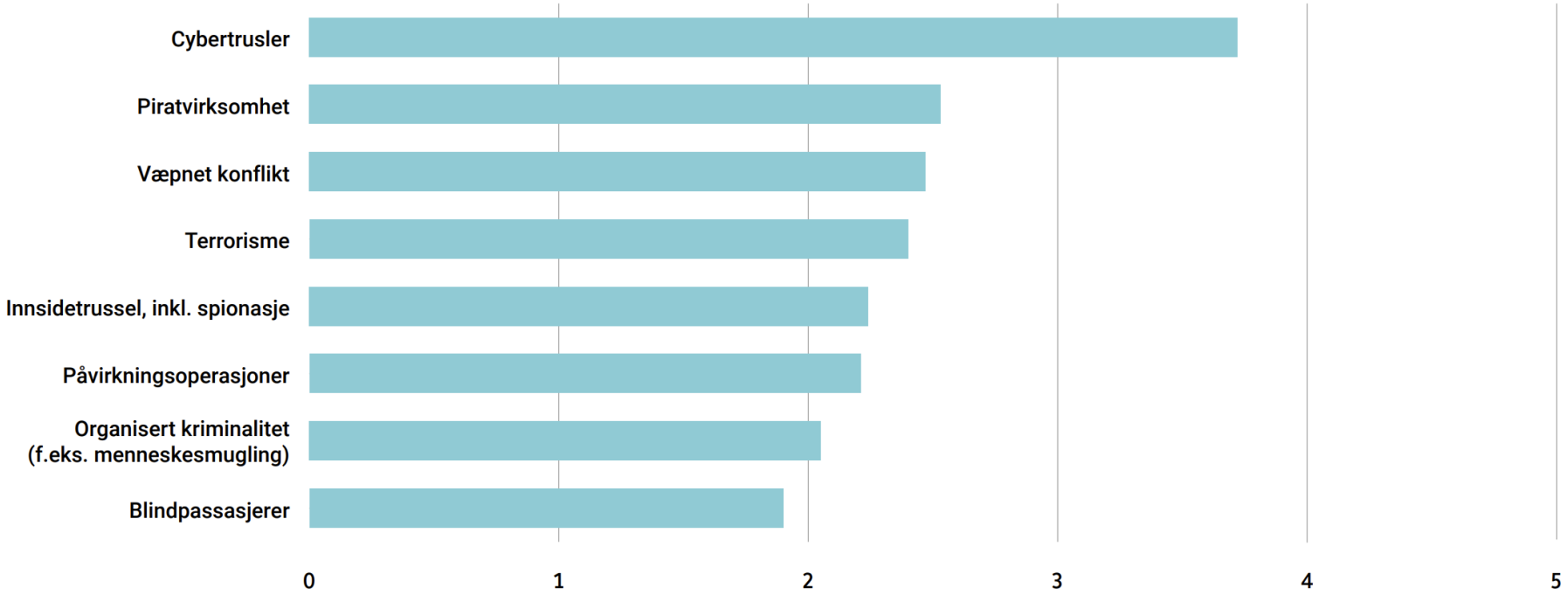
110 members – 2 257 vessels

Maritime Vendor Members:


Does the management really care about cyber risks?

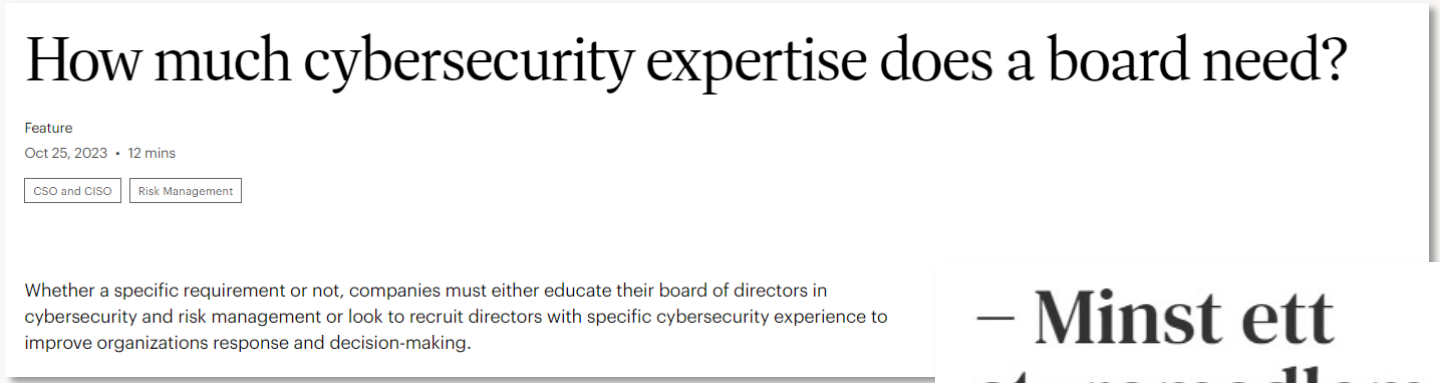
Sikkerhetstruslers påvirkning på rederienes virksomhet

Skala fra 1–5 hvor 1 = ingen grad, 5 = svært stor grad



Kilde: BDO AS/Norges Rederiforbund

Top management cyber security skills



How much cybersecurity expertise does a board need?

Feature

Oct 25, 2023 • 12 mins

CSO and CISO | Risk Management

Whether a specific requirement or not, companies must either educate their board of directors in cybersecurity and risk management or look to recruit directors with specific cybersecurity experience to improve organizations response and decision-making.

— Minst ett styremedlem bør ha cyber-kompetanse

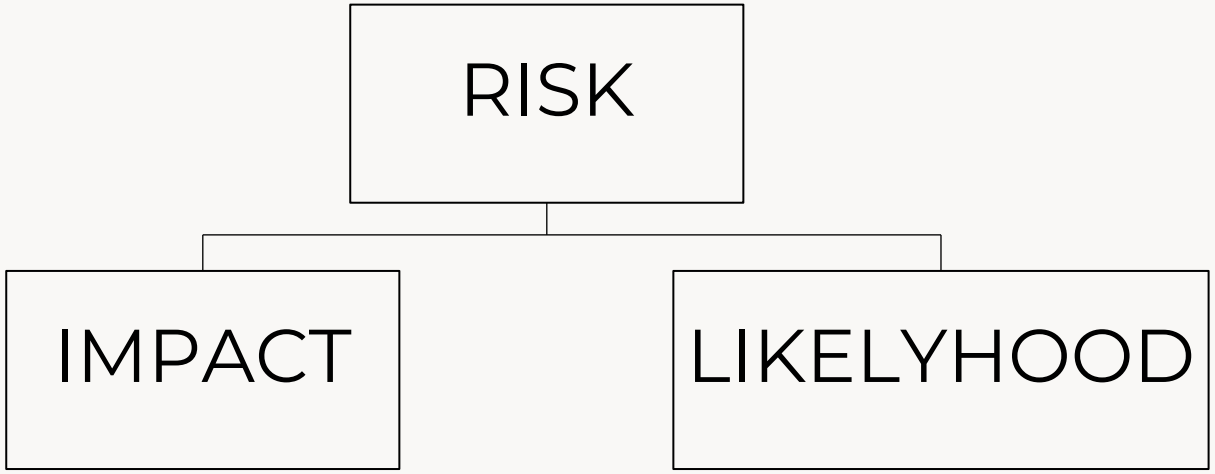
– Cybersikkerhet er like viktig kompetanse i et styre som kunnskap om teknologi og finans. Dette er et altfor komplisert felt til at virksomheter kan sette det bort eller delegere det til lavere nivåer.

How to communicate cyber risks to top management?

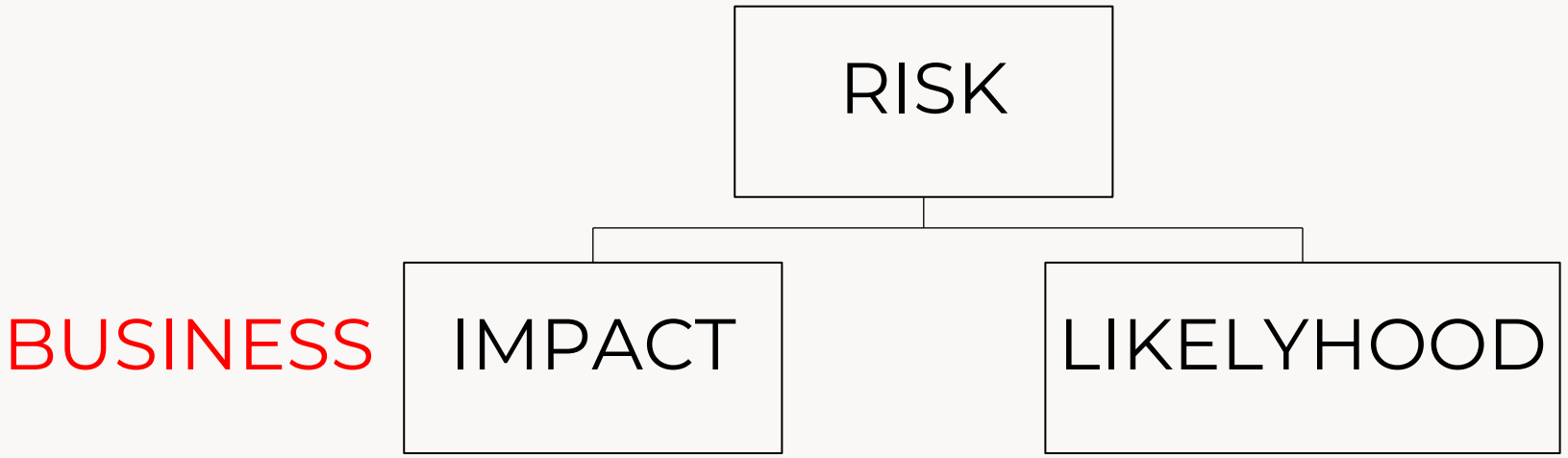
SECURITY RISK ASSESSMENT

RISK

SECURITY RISK ASSESSMENT



SECURITY RISK ASSESSMENT



BUSINESS IMPACT ASSESSMENT

Sit down with the management team and:

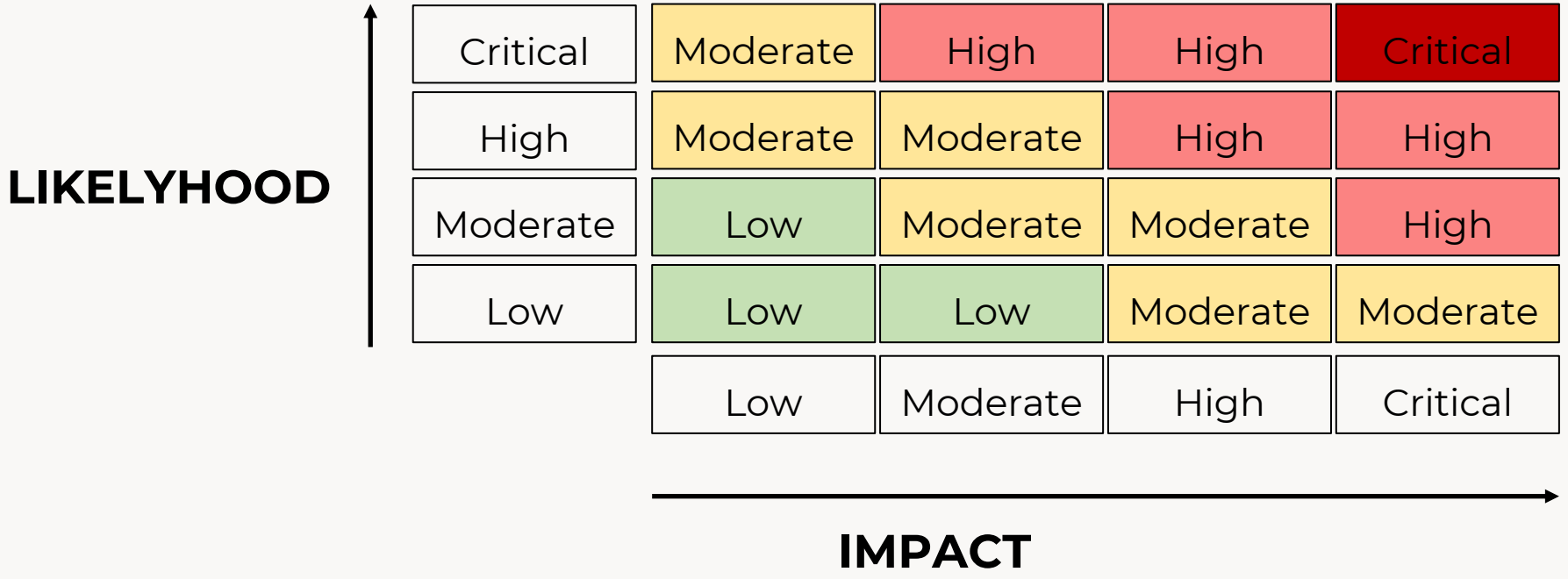
1. List your digital processes supporting your operations
2. Rate how critical each process is in case it is interrupted
3. May use CIA
    1. Confidentiality
    2. Integrity
    3. Availability

4. If little time – define the impacts and then just let the management score the impacts 1 to 4

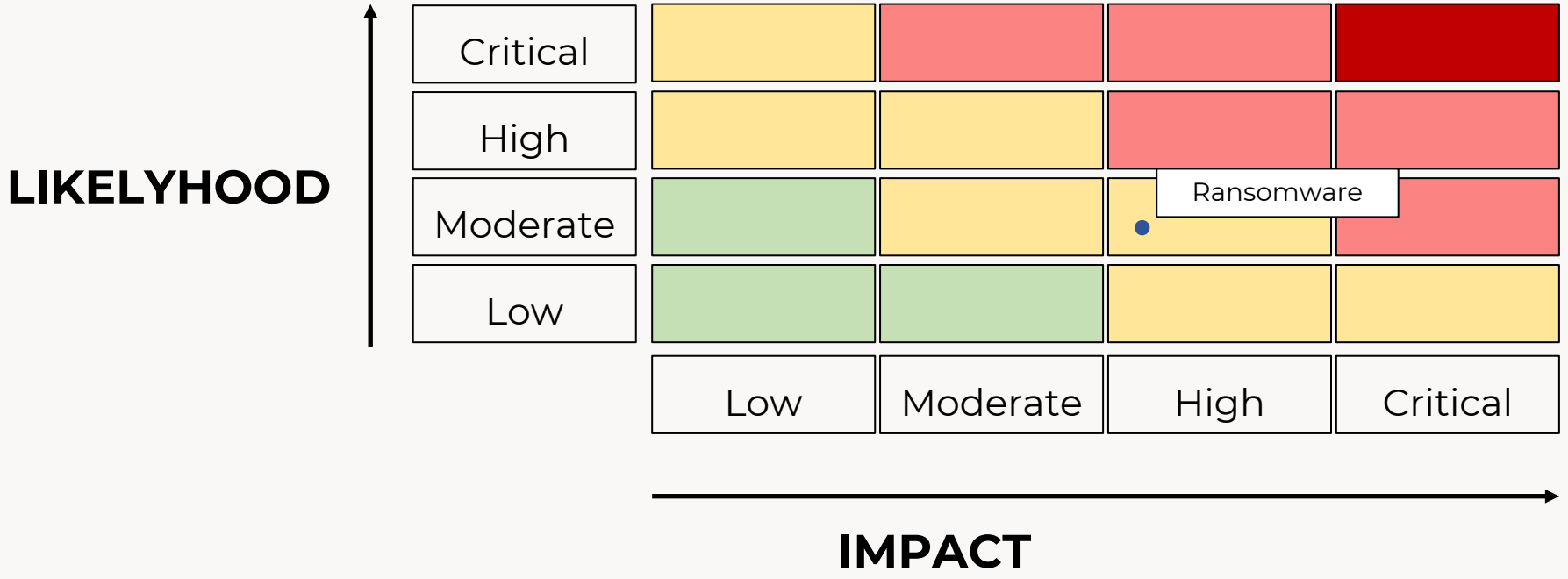
BUSINESS IMPACT ASSESSMENT

1	Theft of business critical information	High
2	Collision, grounding or spill incident caused by destructive cyber attack	Critical
3	Loss of access to critical systems	High
4	Reputational loss	Moderate
5	Sensitive data leaked online	High
6	Financial Loss – fraud	Moderate
7	Webpage not operational	Low
8	Manipulation of content on webpages	Moderate

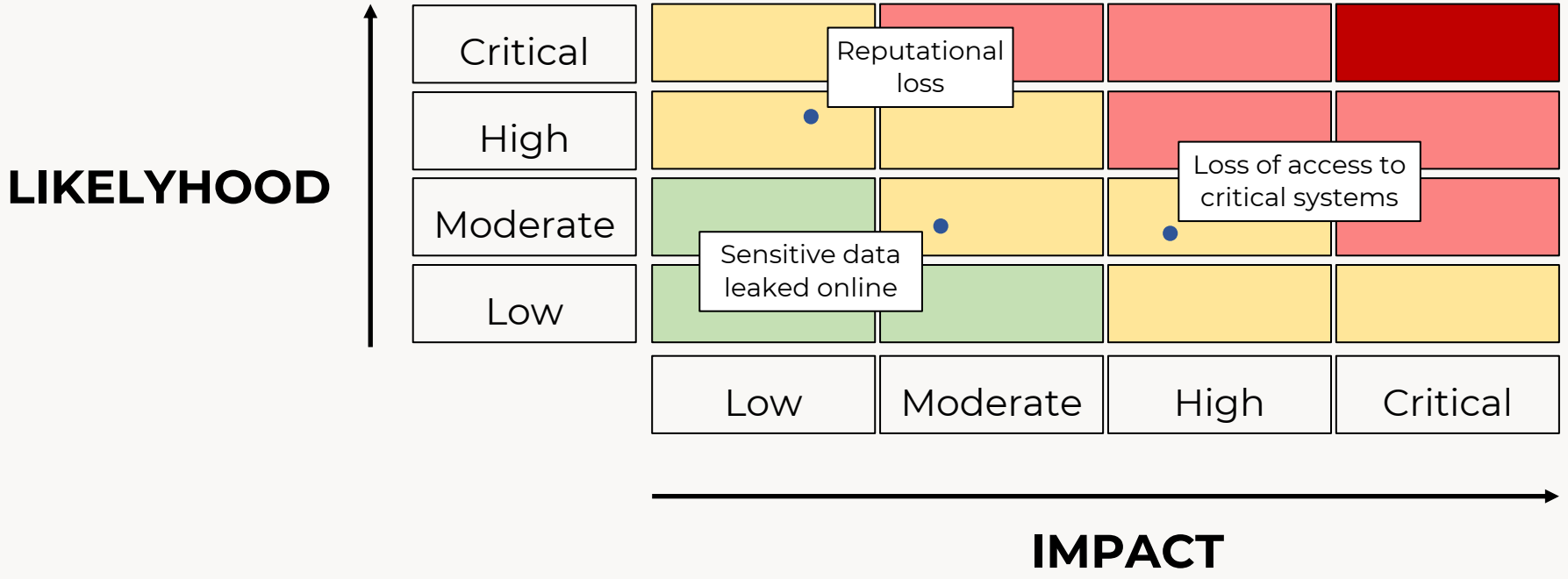
SECURITY RISK ASSESSMENT



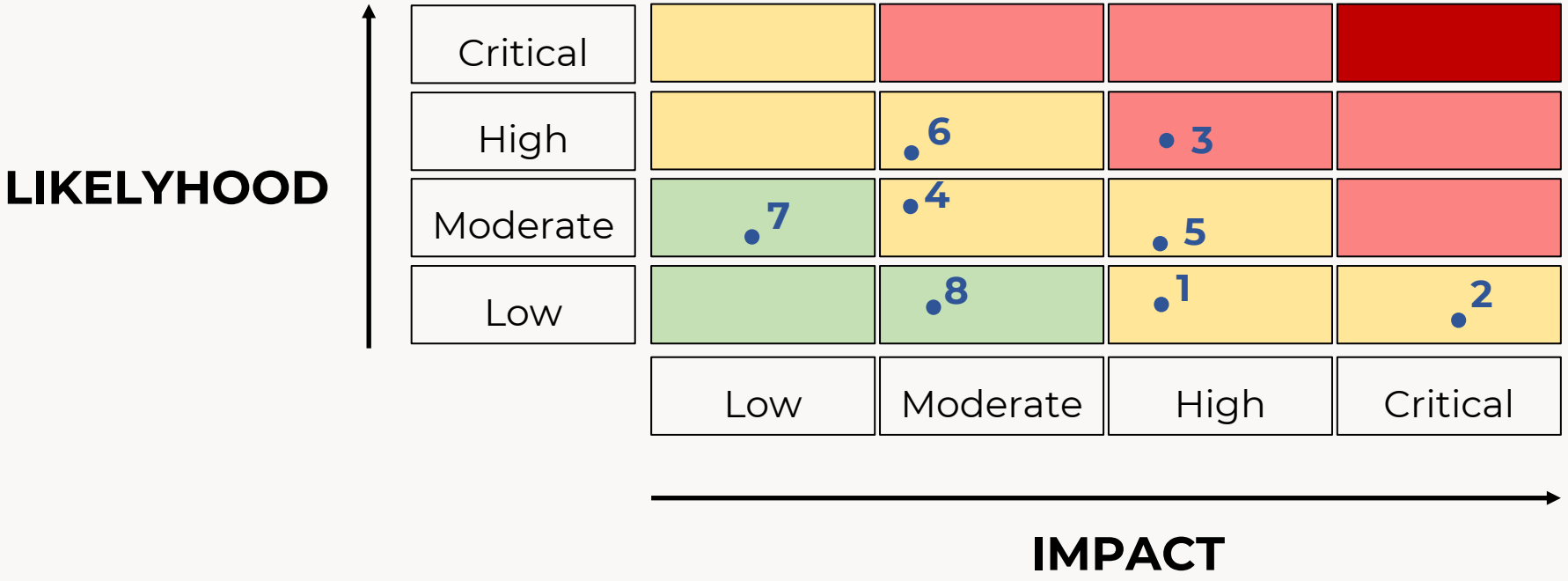
Example - Ransomware



Example - Ransomware



Example – Cyber threats



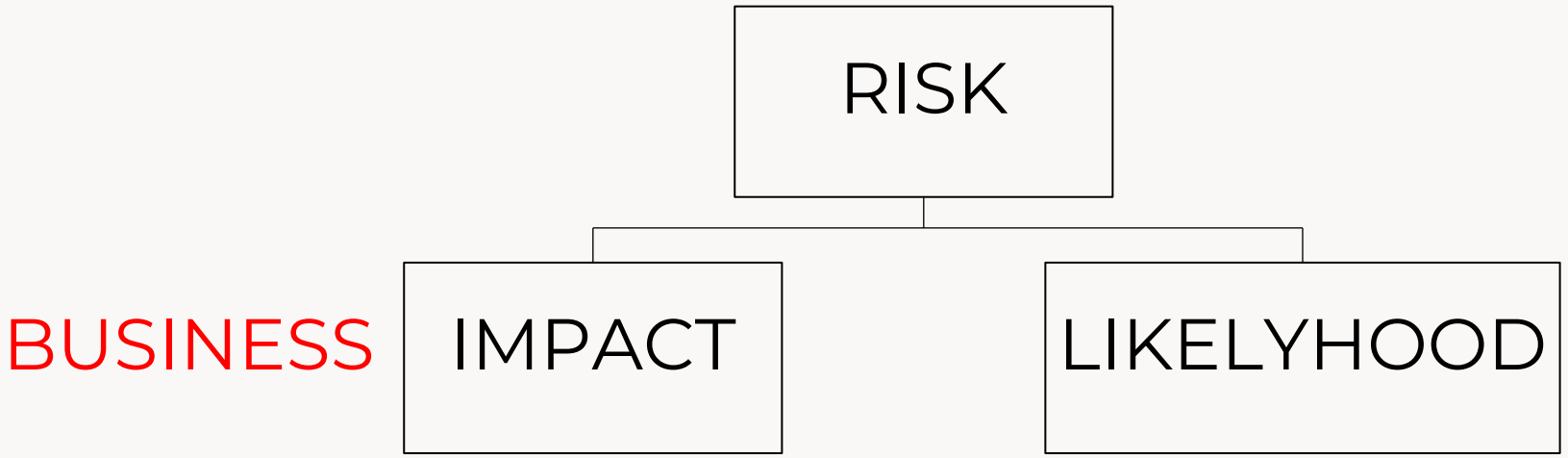
Nation state

Cyber criminals

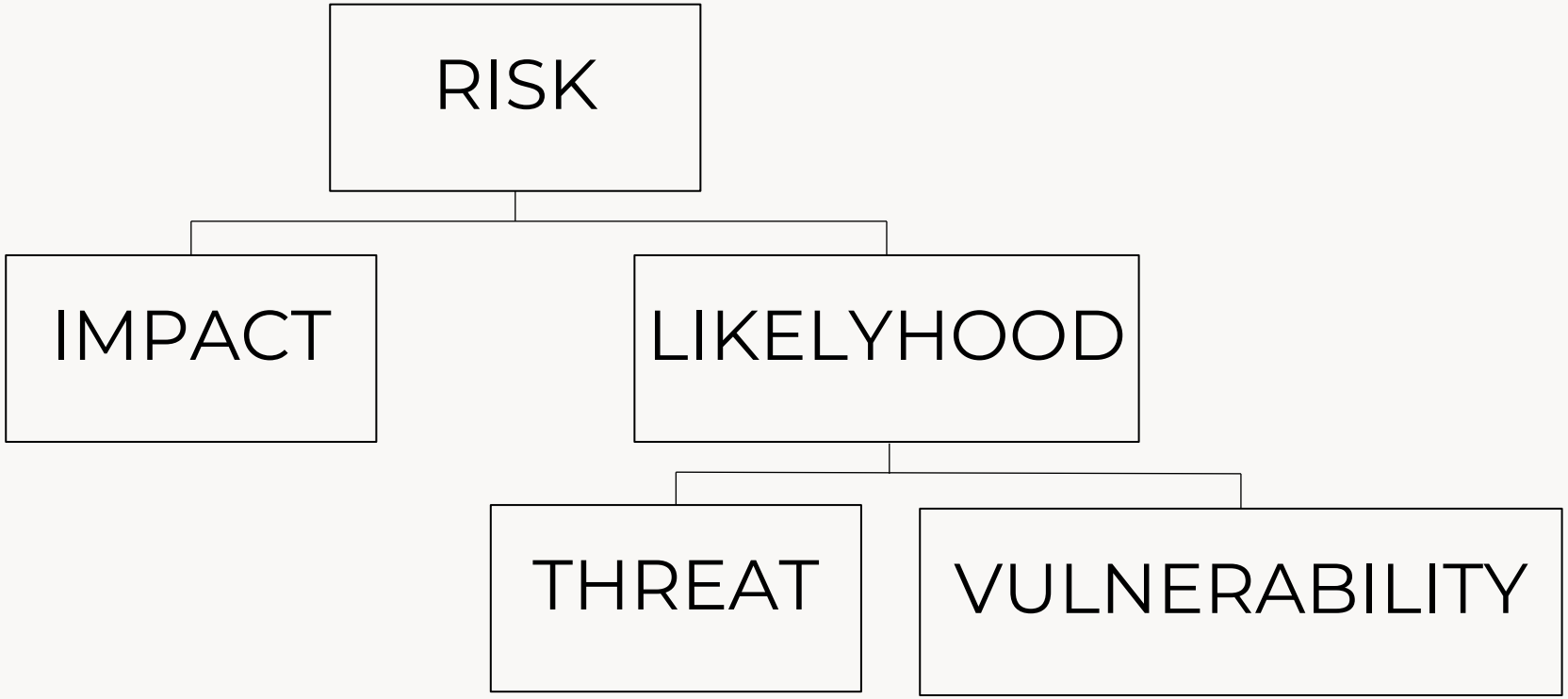
Cyber activists

1	2	3	4	5	6	7	8
Theft of business critical information	Collision, grounding or spill incident caused by destructive cyber attack	Loss of access to critical systems	Reputational loss	Sensitive data leaked online	Financial Loss – fraud	Webpage not operational	Manipulation of content on webpages

SECURITY RISK ASSESSMENT



SECURITY RISK ASSESSMENT




So, what to do if you don’t have management attention yet?

Run a tabletop exercise

- Realistic scenario – something that has happened to other companies similar to yourself.
- Focus on the business impact/implications – not on the technical measures
- How do you manage reserve solutions, internal communication, media handling, clients and stakeholder management, legal aspects?

Summary

- Focus the communication more on business impact/consequence and less about the technical vulnerabilities and threats
- The magic happens when the technical team sit together with the management team and defines the impact/consequence
- Let the management team define/score the business impacts
- Then you focus on minimizing and monitoring the likelihood
- Communicate consistently Risk = Impact x Likelihood (threat x vulnerability)
- Exercise Exercise Exercise!

Contact information

NORMA Cyber OPS:
ops@normacyber.no

24/7 Incident and Crisis number: +47 90 98 97 37

Administrative queries:
contact@normacyber.no

NORMA CYBER

Questions?