

# Incident Response: How to get others in the organisation to care?

Živilė Nečejauskaitė



## Marketing psychology

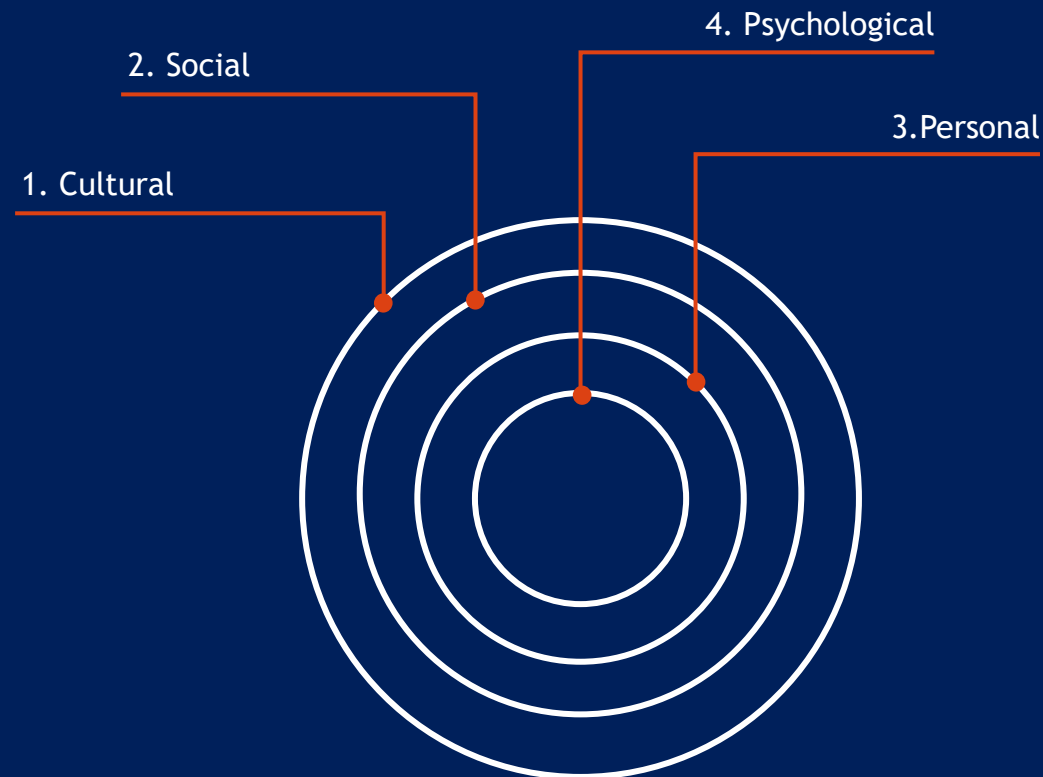
- Michael E. Porter, an American businessman and professor at Harvard Business School
- One of the most well-known marketing minds in the 21<sup>st</sup> century
- Strongly argued that getting information “out there” is not enough to change how somebody feels about it or acts upon it

*Disclaimer: The image is only illustrative and has been created using AI to bring the story moment to life*

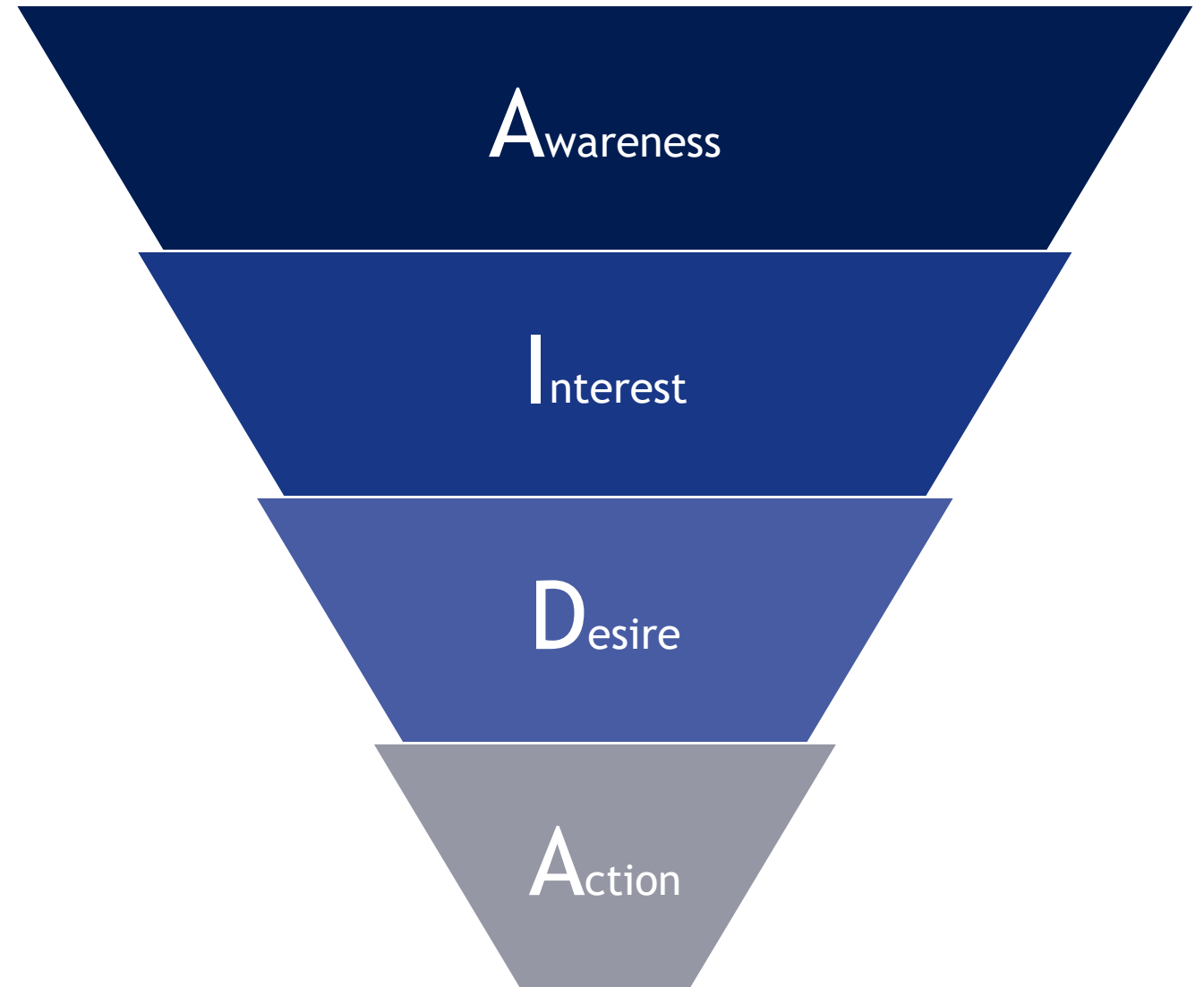


# Marketing psychology

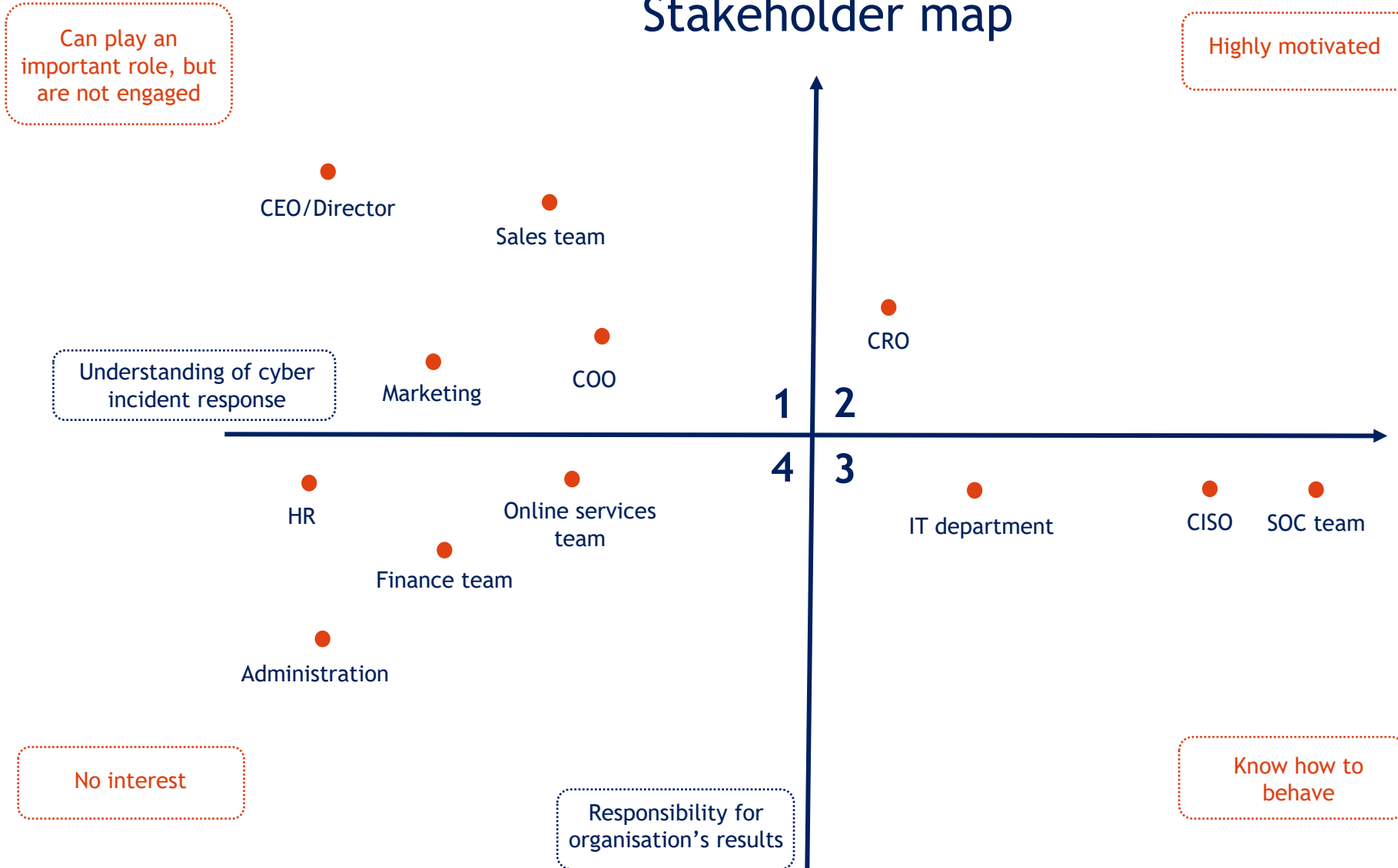
- Marketing is very much based on behavioural economics - it is about predicting behavioural patterns.
- We are more predictable than you think!
- Factors influencing our behaviour:



## Changing perceptions and/or behaviours

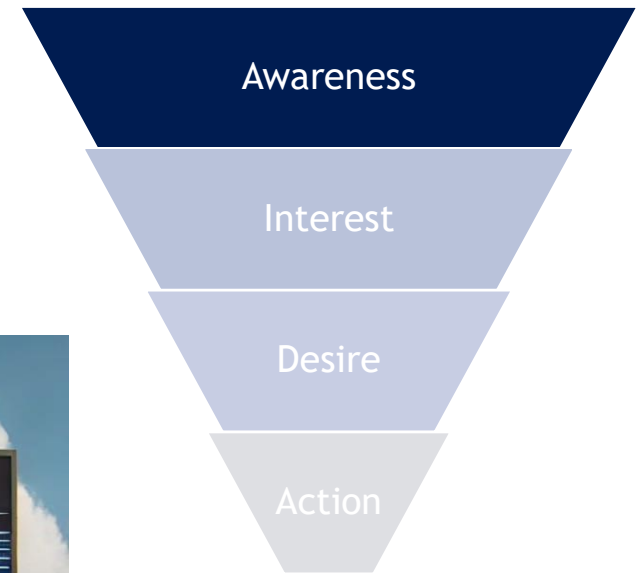
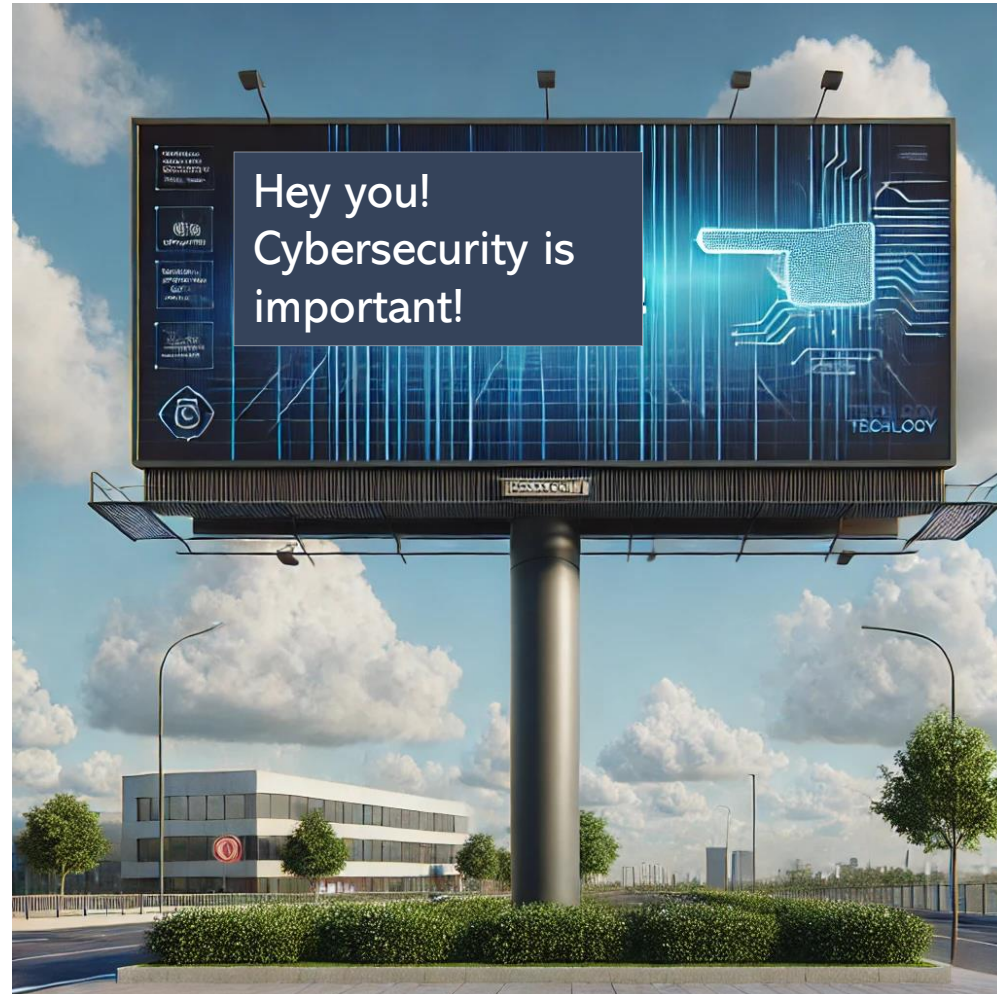


# Stakeholder map



## Get others to know about it

- Clear message
  - How to recognise cyber incidents
  - What immediate actions to take
  - Where and how to report them
- Variety of communication channels
- Reinforcement
- Get help



## The expectancy theory

- Suggested by an American businessman and professor at Harvard Business School Victor H. Room
- The behavior selection is determined by the desirability of the outcome
- Expectancy theory has three components:
  - Expectancy: effort  $\rightarrow$  performance (E $\rightarrow$ P)
  - Instrumentality: performance  $\rightarrow$  outcome (P $\rightarrow$ O)
  - Valence: V(R) outcome  $\rightarrow$  reward

*Disclaimer: The image is only illustrative and has been created using AI to bring the story moment to life*

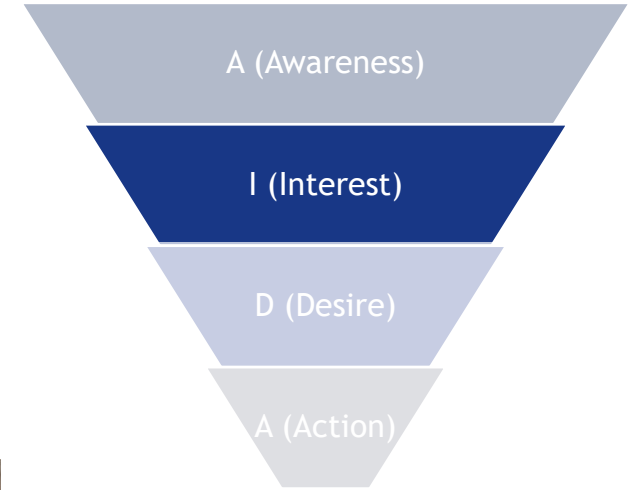


# Get others interested in incident response

**Carrot**

vs.

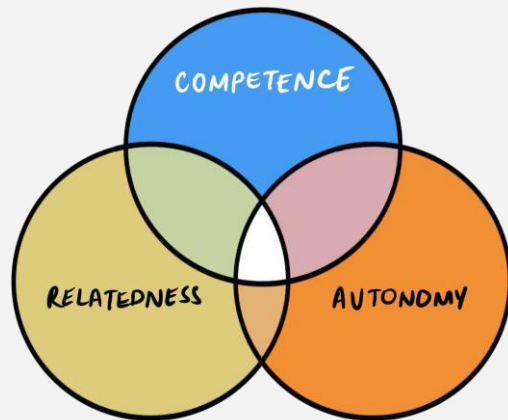
**Stick**





## The self-determination theory

- Mostly attributed to Edward L. Deci and Richard Ryan
- Intrinsic motivation - initiating an activity because it is interesting and satisfying in itself to do so



*Disclaimer: The image is only illustrative and has been created using AI to bring the story moment to life*



## So why others might change their behaviours?

### Motivation

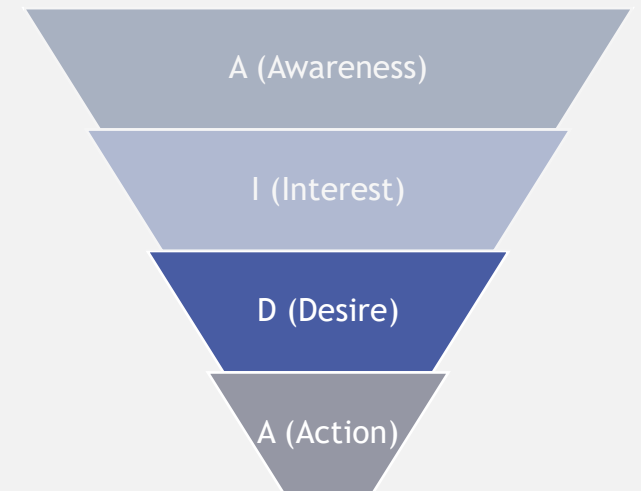
- I understand why it is important
  - Self-determination
  - Subjective norms
- I care about this organisation
- It concerns me - my personal data
- It concerns something I am responsible for, e.g., customer data (my job is at risk)

### Methods

- I take an active part
- I am part of the process

### Advocates

- I truly believe in the value it brings
- It is part of my daily/periodical conversations I engage in



## NRD Cyber Security example #1

- Simulation of a cybersecurity incident: data breach
- All day exercise

**From:** SunjivPartel <[SunjivPartel@proton.me](mailto:SunjivPartel@proton.me)>  
**Sent:** 16 December 2024 14:38  
**To:** [REDACTED]  
**Subject:** YOUR NETWORK HAS BEEN BREACHED

**EXTERNAL**

After one of your colleagues opened an enticing attachment, we have successfully penetrated your network and gained full access to your systems:

- Financial records
- Client and employee information
- Proprietary business data
- Email communications and confidential contracts

In addition to data theft, we have encrypted all files on your network, rendering them inaccessible without our decryption software.

**What You Need to Know:**

1. **Your sensitive data is at risk of public exposure.** If our demands are not met, the data will be leaked or sold to interested parties.
2. Backups have been accessed and compromised, and shadow copies have been removed. Recovery is not possible without our assistance.
3. Attempts to recover files or contain the breach without cooperation will result in immediate publication of your stolen data.

Cybersecurity incident may have been over  
but crisis situation was not closed yet -  
discussions on media monitoring

## Process



Emails to [info@nrdfs.lt](mailto:info@nrdfs.lt) about the attack



Phone calls by “journalists” to our info line



Phone calls by “journalists” to specific people

## Result



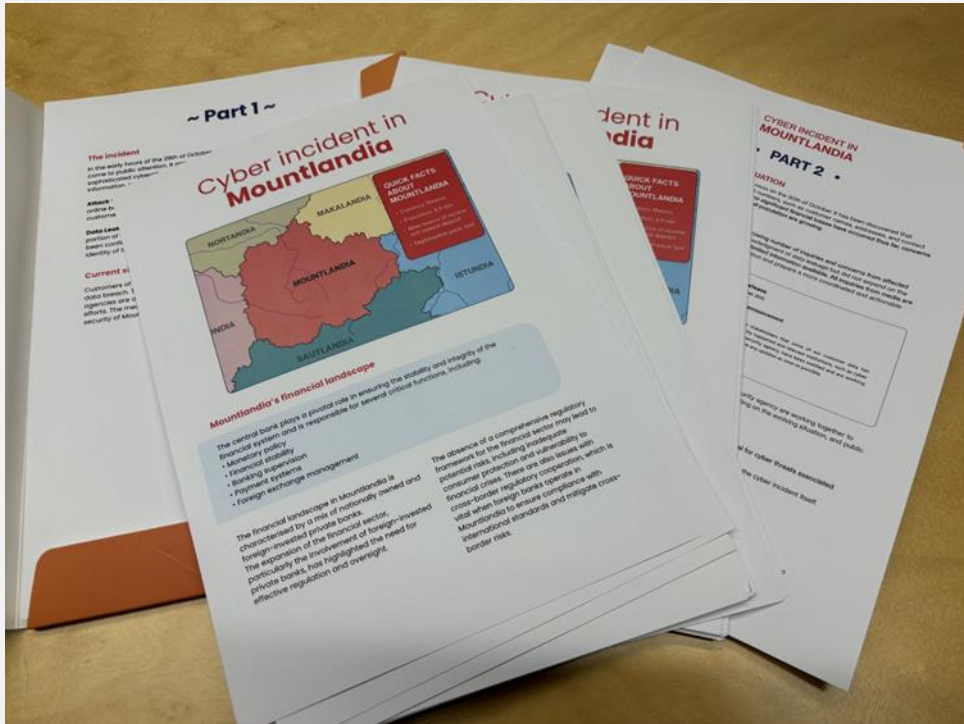
The “button” was pressed, and we had an emergency meeting, BCP was activated



Continuous updates, meet-up at the of the day to discuss progress and next actions

# NRD Cyber Security example #2

Tabletop exercise (TTX)



## How it works?



Fictional, yet realistic scenario



Cybersecurity focused, but is not centered around cybersecurity team



Requires active participation of all attendees

## What it brings?



Engaging as it has gamification elements, thus the scenario is progressing



Empowerment: the participants take actions that have direct results

Thank you