Communicating in the eye of the storm: Dos and Don‘ts for cyber crisis communications

Dominic Bertram, ISSS Conference Berne, 11.01.2023

DETECON
CONSULTING

Crisis communications is difficult – even more so after a cyber attack

What constitutes a crisis?

- A crisis is the perception of an often unpredictable, unexpected event that threatens to disrupt an organization’s assets and negatively affects their bottom line
- Stakeholders are at the center. Their expectations and perception influences the course of the crisis

Technical language & complexity

Communicating the technological context and the technical origins of the crisis and making it accessible and understandable for all is hard

Time-lag between attack and discovery

The time-lag between the attack and the discovery can influence the perception of the organization (allegedly 207 days for data breaches*)

Regulatory requirements and legal liability

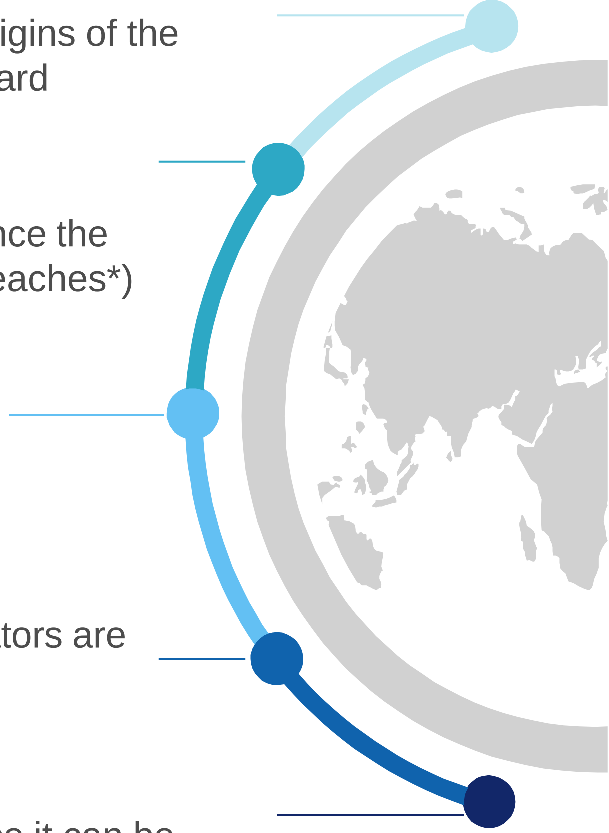
Regulatory requirements to communicate if certain data elements are affected

Uncertainty & attribution

The cause of the crisis is not known, the attackers or perpetrators are difficult to identify

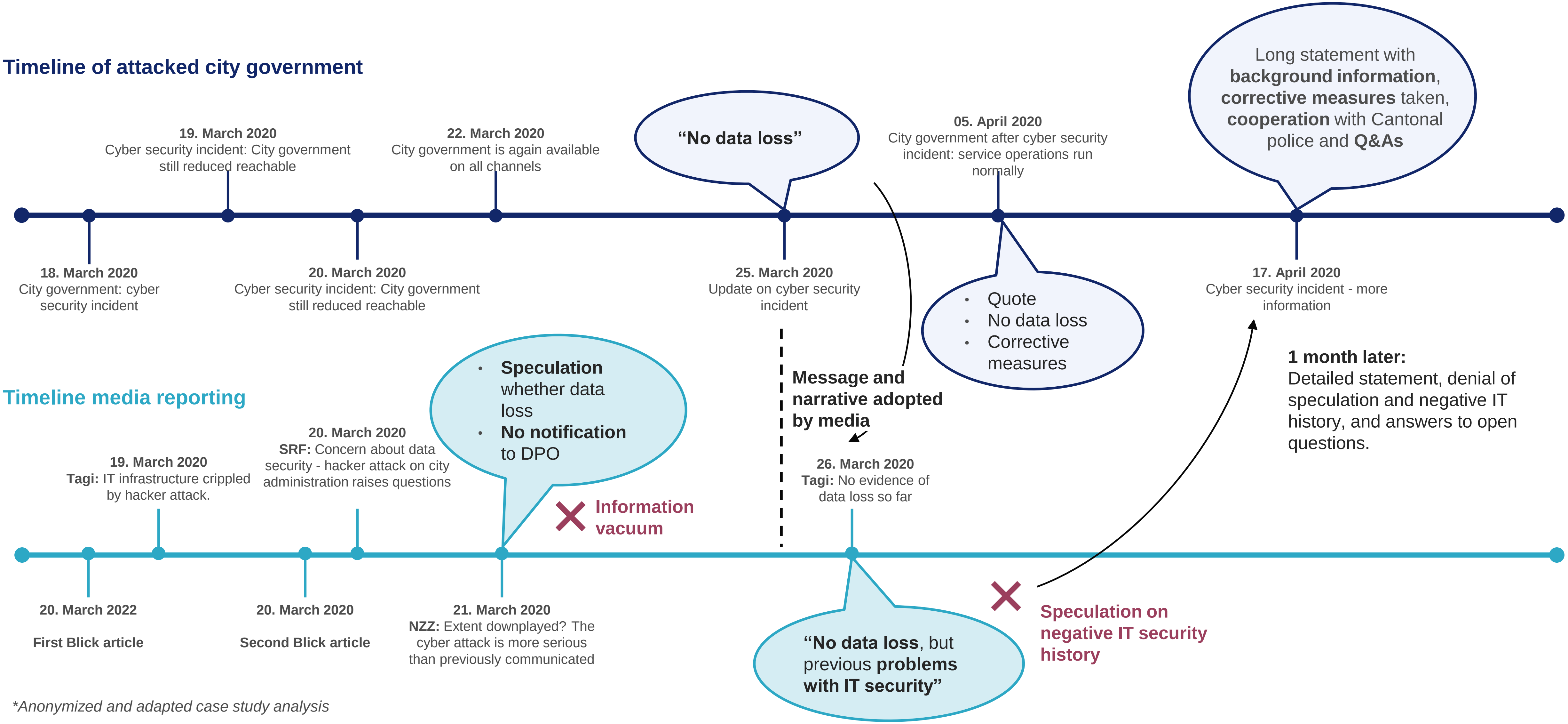
Wrong incentives

Organizations have an incentive to keep the crisis hidden since it can be invisible to outsiders



*Source: https://www.ibm.com/reports/data-breach

Case study: the hacking of a city government



Timeline of attacked city government

18. March 2020
City government: cyber security incident

19. March 2020
Cyber security incident: City government still reduced reachable

20. March 2020
Cyber security incident: City government still reduced reachable

22. March 2020
City government is again available on all channels

25. March 2020
Update on cyber security incident

“No data loss”

05. April 2020
City government after cyber security incident: service operations run normally

- Quote
- No data loss
- Corrective measures

17. April 2020
Cyber security incident - more information

Long statement with **background information**, **corrective measures** taken, **cooperation** with Cantonal police and **Q&As**

1 month later:
Detailed statement, denial of speculation and negative IT history, and answers to open questions.

Timeline media reporting

20. March 2022

First Blick article

19. March 2020
Tagi: IT infrastructure crippled by hacker attack.

20. March 2020

Second Blick article

20. March 2020
SRF: Concern about data security - hacker attack on city administration raises questions

21. March 2020
NZZ: Extent downplayed? The cyber attack is more serious than previously communicated

- **Speculation** whether data loss
- **No notification** to DPO

✕ **Information vacuum**

Message and narrative adopted by media

26. March 2020
Tagi: No evidence of data loss so far

“No data loss, but previous **problems with IT security”**

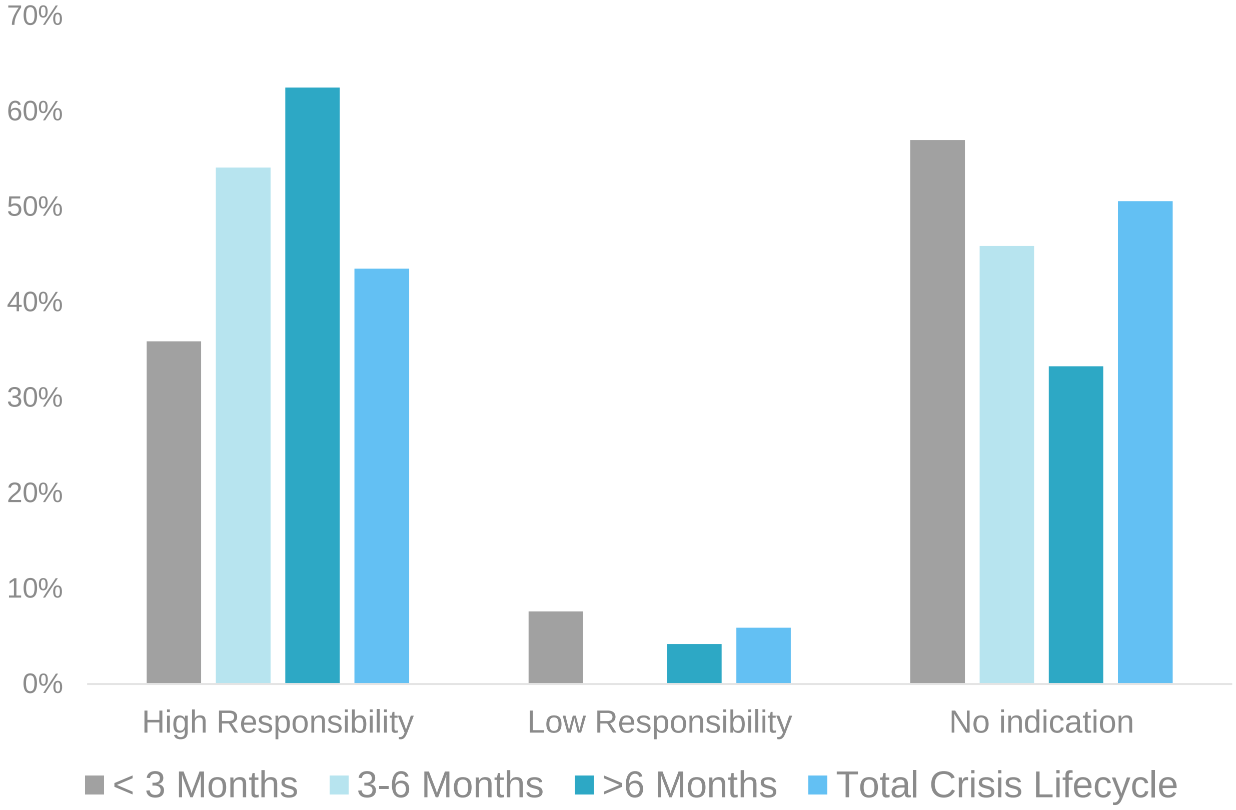
✕ **Speculation on negative IT security history**

*Anonymized and adapted case study analysis

DETECON CONSULTING

Perception of crisis responsibility by media outlets

Organizational responsibility attribution by media outlets after data breaches caused by cyber attacks



Dominic Bertram, 2021, Crisis Communications after Data Breaches (unpublished)

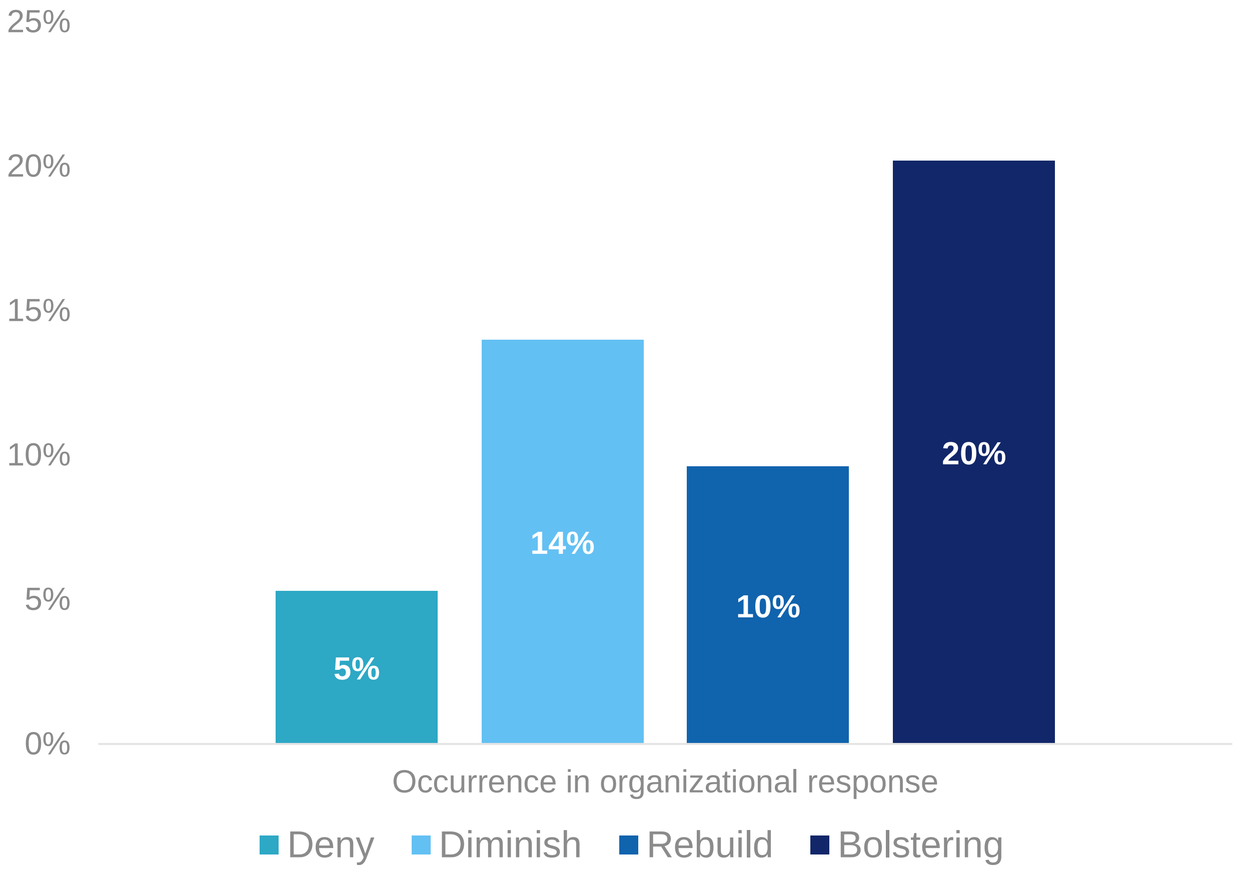
- The public assigns **high levels of responsibility to the organizations** involved in cyber incidents
- **Similar crises in the past reinforce this effect** and undermine the trust of stakeholders
- Affected organizations should therefore **accept responsibility and communicate accordingly**

Data sampling and analysis:

- *255 articles on four different cases*
- *from three different geographic regions (U.S., U.K., and Germany)*
- *from a basket of daily online and print outlets (conservative, centrist, progressive)*
- *no Social Media included*

Perception of crisis responsibility by media outlets

Identified crisis response strategies after cyber attacks resulting in data breaches



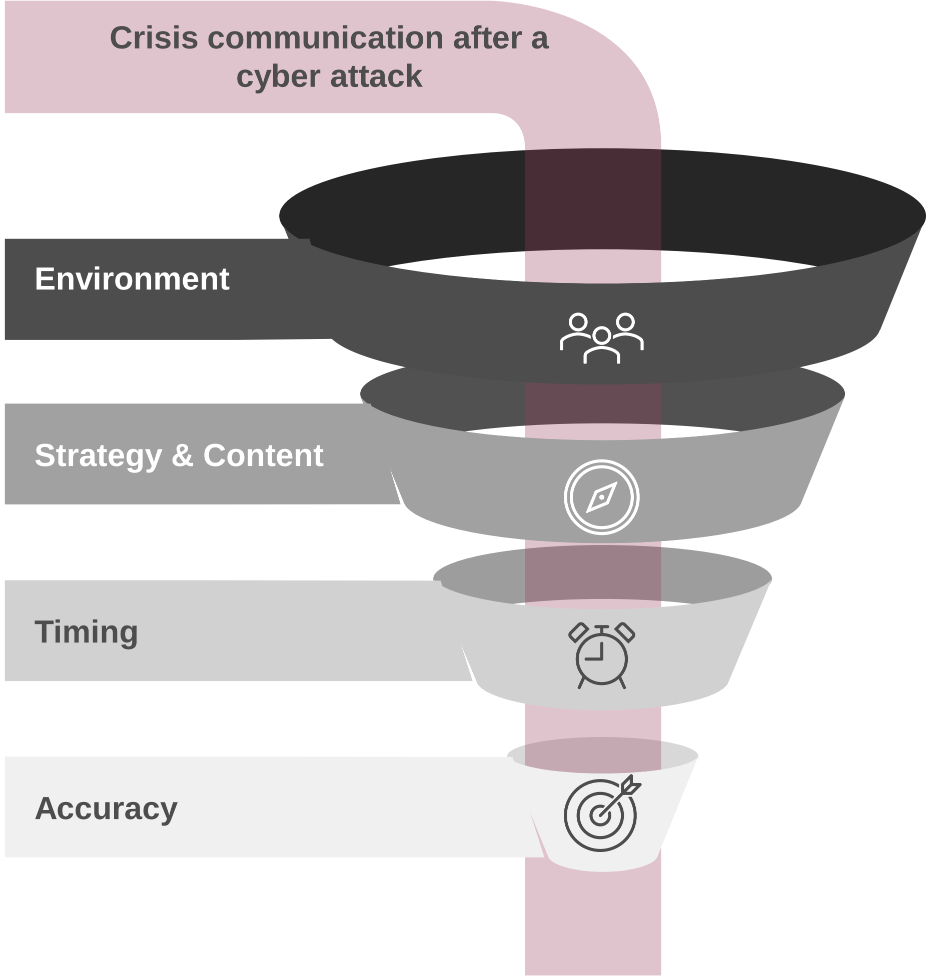
Dominic Bertram, 2021, Crisis Communications after Data Breaches (unpublished)

- Organizations still **portray themselves as victims**
- They combine this **with diminishing the crisis** (playing it down)
- From the media data, we interpret that **these are the wrong strategies to resolve a crisis**

Data sampling and analysis:

- *Four cases of cyber attacks resulting in data breaches*
- *114 Crisis response documents (media release, e-mail, website communication)*
- *Only written and no oral statements analyzed*
- *No Social Media posts analyzed*

The Don’ts – what to avoid in cyber crisis communications



1. Don’t ignore your stakeholders needs and their perception
2. Don’t try to hide the attack – someone else will out you
3. Don’t portray yourself as the victim
4. Don’t diminish the cyber attack by playing it down
5. Don’t delay your incident response artificially
6. Don’t create an information vacuum

The “Do’s” – good practices in cyber crisis communications

1 Know your stakeholders and how to communicate with them

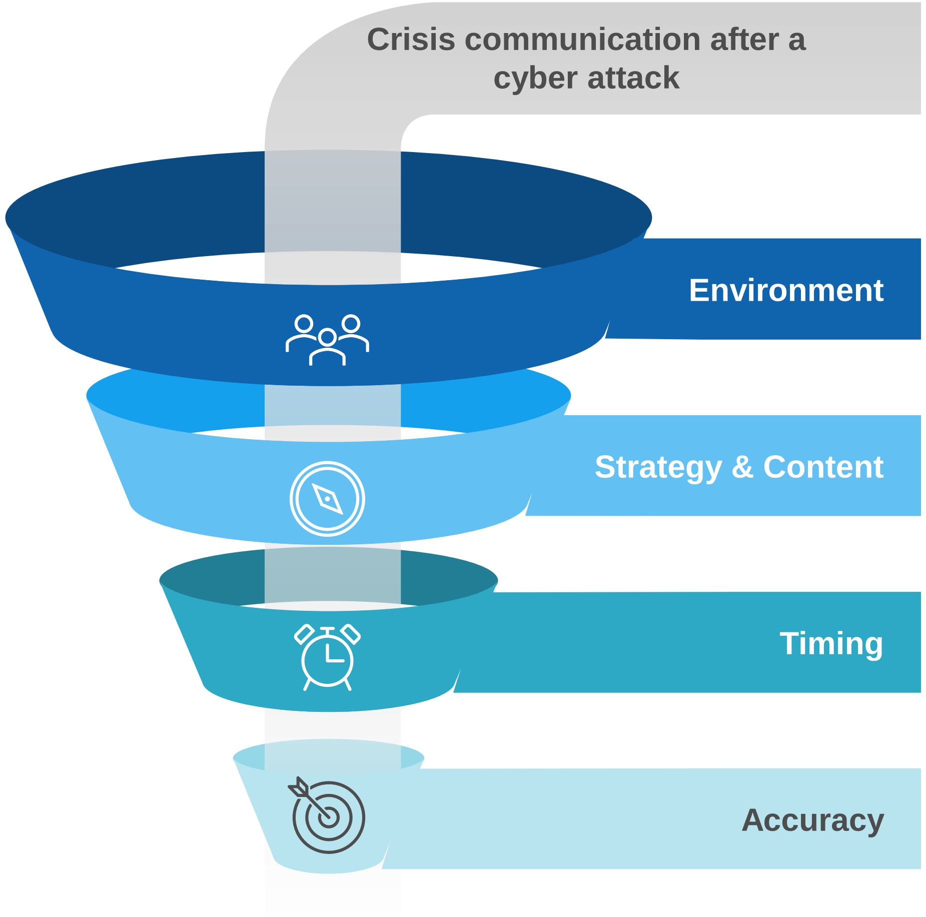
2 Know the regulatory environment & notification requirements

3 Chose accommodative strategies by taking responsibility

4 Build trust by communicating corrective measures

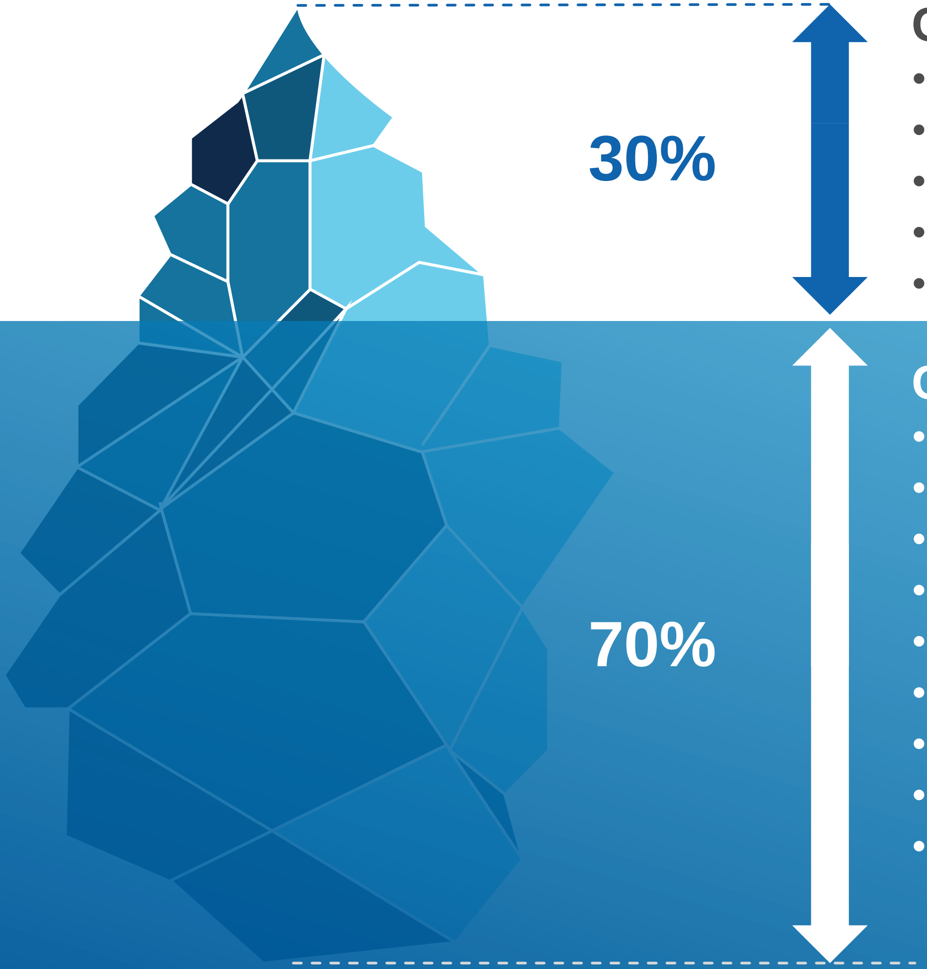
5 Communicate timely and be proactive

6 Be transparent and know your track record



How can crisis communications contribute to resilience?

Crisis communications forward planning enables organizations to adapt and respond coherently in a coordinated way



Crisis Response & Execution

- Adjust and execute the communication plan to current situation
- Communicate timely with pre-written content
- Chose appropriate channels and messages for different stakeholders
- Communicate accurate and timely
- Include feedback and iterate

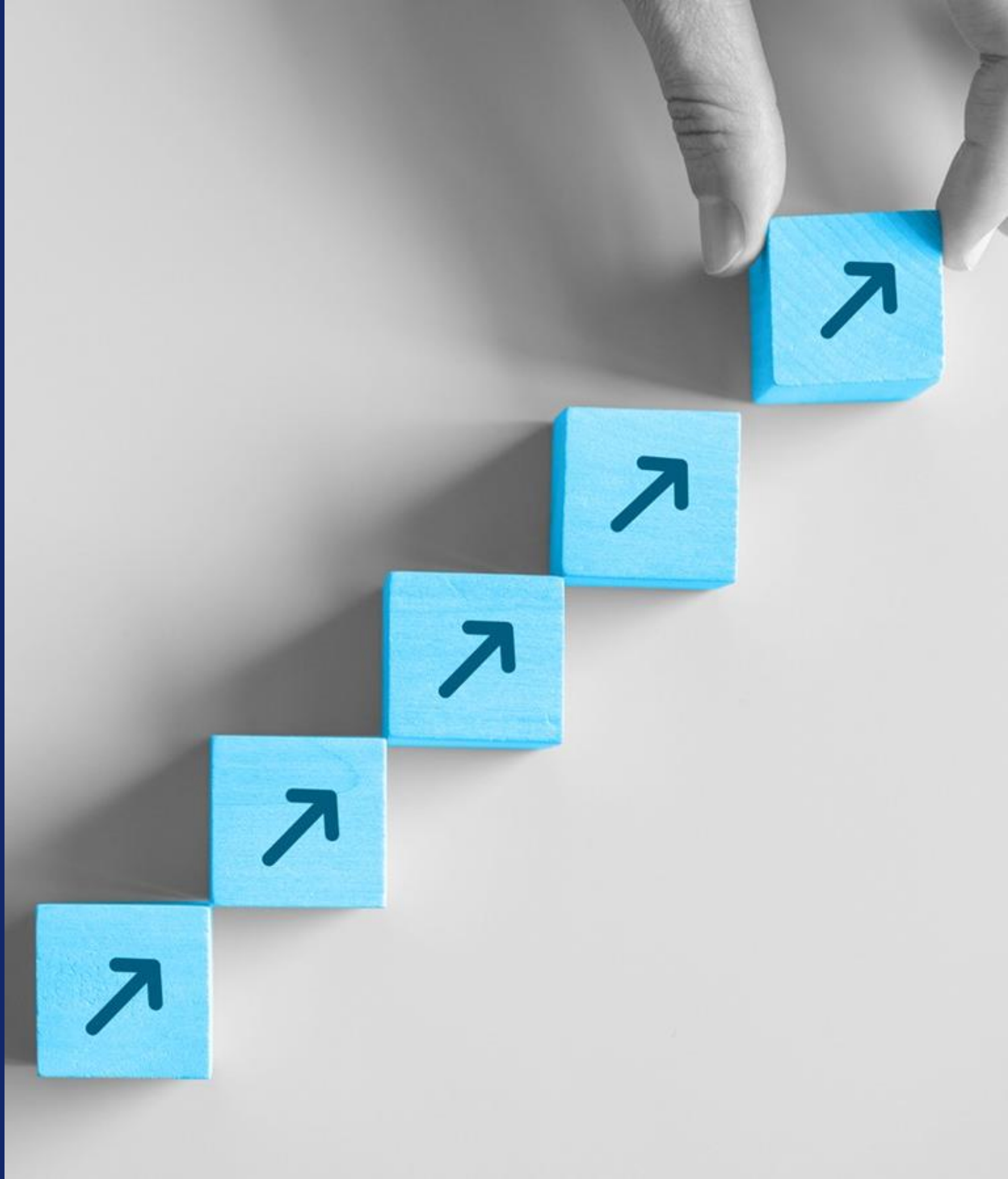
Crisis Communications Preparation

- Break up silos between Security, IT, Legal and Communications
- Have a stakeholder map at hand
- Build communication plans with different scenarios
- Establish clear responsibilities and processes
- Brief your security team what information the communications team need
- Pre-write common Q&As and holding statements
- Ensure redundant communication channels in case of cyber attack
- Build a framework for effective communications with impact spheres
- Train, get feedback and optimize

Thank you.

Dominic Bertram
Detecon (Schweiz) AG
Löwenstrasse 1
8001 Zürich

Mobile: +41 79 414 72 09
Email: dominic.bertram@detecon.com



DETECON
CONSULTING