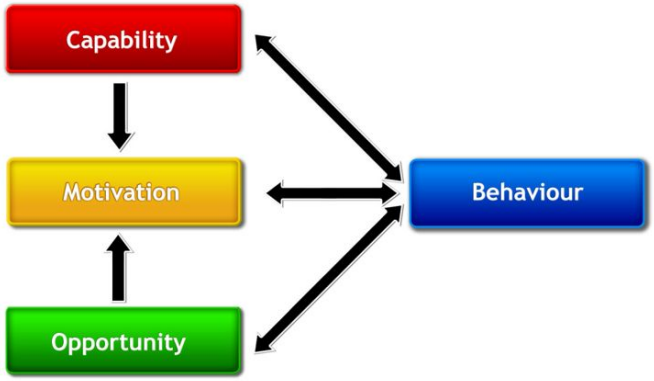
Shapiro V.

COM-B framework and behavior intervention design for business policy makers related to digital security.

Digital or cyber security is the hottest topic in today's media. Every day we hear more about another data breach and another set of private information exposed. Some of the reasons why breach happened are purely technical, but most of the problems lie in human behavior. Cyber security subject matter experts, pure researchers and seasoned practitioners are talking about human factor.

All of these studies are focused on regular users, as I called them in my Costidity study, "policy constituents". Specialists discuss how to make them better in day-to-day "security hygiene", how to recognize phishing emails, how not to open suspicious attachments, etc. We also refer to company leadership to pay more attention to cyber security issues and change atmosphere in the organization by making users part of the solution, not the problem. Both of the approaches require changes people's behavior, even after they've got the knowledge.

In [1], authors proposed a new behavior intervention model called COM-B:



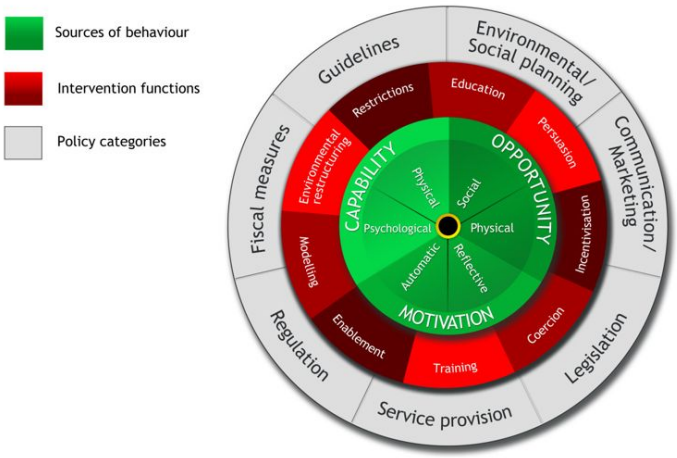
If we want to change someone's behavior, we should create a motivation via new opportunity or/and new capability: "Applying this to intervention design, the task would be to consider what the behavioural target would be, and what components of the behaviour system would need to be changed to achieve that."

Other authors ([3], [4]) applied this model for user behavior and worked on how to design behavior intervention for them. I would like to expand this approach to

policy makers (owners of digital security policies) and policy enforcers (see [2]).

Here is the list of discussion topics:

- COM-B behavior intervention design for policy makers: what works, what does not work in real life.
- My top 10 human factor questions for policy makers:
    - What is the final specific people-centric goal of the policy?
    - How does policy implementation process look like?
    - What is the time/productivity penalty for the organization after policy becomes mandatory?
    - What is real aptitude of potential constituents towards the policy?
    - What is real aptitude of potential enforcers towards the policy?
    - What are the incentives for policy constituents to follow it?
    - What are the incentives for policy enforcers to enforce it vs. ignore it?
    - What is the process of handling policy exceptions on human level?
    - What is the process of managing/mitigating policy violations?
    - Who is responsible for policy governance?
- Using behavior change wheel for behavior intervention of policy makers and policy enforcers:



Literature:

1. Susan Michie, at el: “The behaviour change wheel: A new method for characterising and designing behaviour change interventions”. Implementation Science2011, https://doi.org/10.1186/1748-5908-6-42
2. J. Baldini, V. Shapiro: “Costidity: The Cost of Human Factor”, 2015
3. Adam Joinson: “Behaviour change, Cyber Security and Lessons from other domains”, University of Bath, #CYBERUK 2017

4. John Blyth, Cameron Lefevre: “Why psychology could be the answer to cyber-attacks”, https://www.weforum.org/agenda/2016/11/why-psychology-could-be-the-answer-to-cyber-attacks