Framework proposal

Four high level grand challenges

- Design driven by people/organizations/society capabilities/needs.
- Cybersecurity that is visible, understandable, controllable, and manageable
- Understanding and combatting criminal element and state actors
- Cybersecurity seen through a chaotic lens

[Original] How do we design, build, evaluate, and maintain secure cyberinfrastructure that incorporate social, technical, and human aspects?

[Definition - Wikipedia]

United States federal research funders use the term **cyberinfrastructure** to describe research environments that support advanced data acquisition, data storage, data management, data integration, data mining, data visualization and other computing and information processing services distributed over the Internet beyond the scope of a single institution.

[Revised] Designing and evaluating secure digital infrastructure driven by scientific knowledge of social, technical, and human aspects

[Definition]

A digital infrastructure is an integrated set of technology, systems, tools, policies, and processes that support information services beyond the scope of a single institution.

Example

The man responsible for most of your password headaches was wrong, and he's sorry

1:40 a.m. ET

iStock

In 2003, Bill Burr, a manager at the U.S. National Institute of Standards and Technology, wrote an 8-page paper titled "NIST Special Publication 800-63. Appendix A." That document — which suggested people come up with obscure passwords with capital and lower-case letters plus symbols and change their passwords often — became the cornerstone of corporate password management and internet security conventional wisdom for more than a decade. Now, Burr, 72 and retired, has a confession and an apology, *The Wall Street Journal* reports. "Much of what I did I now regret," he said.

Sub-Challenges

- Map and model cybersecurity risks faced by individuals, organizations, and society
- Design and implement cybersecurity frameworks, systems, tools, processes, and policies driven by understanding of technology, human, and society
- Measure, monitor, and evaluate effectiveness of the secure digital infrastructure

Measurable Outcomes

- Qualitative and quantitative models of cybersecurity risk at {individual, organizational, national} level
- Significantly reduced data at breach incidents and costs at {individual, organizational, national} level
- Increased compliance with cybersecurity regulations and policies at {individual, organizational, national} level

1. What is the problem and why is it important?
2. Why is this difficult to do?
3. Why is progress possible?
4. What are the barriers for success?

Grand Challenge

Empower users to make informed security decisions that are visible, controllable, and understandable while maintaining trustworthy and autonomous agency for public discourse

- Problems: Misinformation, insider negligence, insider threats, deceptive/fake public opinions
- Difficult? No ground truth, lack of appropriate understanding of the consequences of security actions, unknown intent
- Progress possible? Identification of cues from the environment
- Barriers:
  - Communicate consequences of security action
  - Investigate ground truth
  - Noisy and complex cues
  - Late discovery of user's or agency's nearly invisible motives

Cybercrime

- Cybercrime Data Grand Challenges
- To be done:
  - i. What is the problem and why is it important? (Material can be harvested from section 1 of the slide-deck)
  - ii. Why is this difficult to do?
  - iii .Why is progress possible?
  - iv. What are the barriers for success?

Cybercrime

- Grand challenge: how do establish the historical record before the data disappears?
- Grand challenge: what data needs to be gathered for effective cybercrime statistics?
- Grand challenge: how to develop effective analytics for cybercrime data?
- Grand challenge: how do we balance privacy with collection and analysis of this data?
- Grand challenge: how can we make the “prosecution paradigm” (from non-cyber crime) effective in the cyber domain---and what are its limits?

Preparing for Chaos

- Suggested Grand challenge: Organizations are incentivized to anticipate and handle cyber crises.
  - Re-Worded: Being able handle the normal chaos of cybersecurity becomes common place.
  - Re-Worded: Organizations are incentivized to anticipate and handle the complexity of cybersecurity.
  - Re-Worded: Organizations are incentivized to anticipate and handle the complexity of cyber crises.
  - Re-Worded: Organizations are incentivized to anticipate cyber crises.
  - Re-Worded: Incentives for anticipating and handling cyber crises is the norm.
  - Re-Worded: Organizations are incentivized to antipate and handle cyber crises.

Preparing for Chaos

- Safety plans often become fantasy plans (Perrow, 1999);
- When emotions take over from our rationality, we forget all the rules (Kahneman, 2011);
- We must accept that we have no control when complexity increases or as Kahneman says, when fast thinking takes over from slow thinking
- How do we cope with this?
  - A chaotic and complex environment impacts operational stability, therefore, organizations must be flexible;
  - If we look at cybersecurity this way, we may be better and adequately prepared when cyber crises happens;
  - If organizations are incentivized (levers and mechanisms) with this lens, they may be more encouraged to better anticipate and handle these events when they happen.
- Some companies are beginning to consider this approach and are standing out from the pack because of it, but it's far from being mature or the norm.
  - - Netflix (Chaos Monkey)
  - - Google (Google Shield)
  - - Microsoft (Fuzzing service)