Summary Report: First Workshop on Cyber Public Health

What we did

On January 9, 2024, CyberGreen and Google co-hosted the inaugural Cyber Public Health (CPH) workshop, an exploration into future directions and research in the field. The hybrid workshop was an opportunity to assess past achievements, introduce fresh perspectives to the discourse, and establish shared objectives for collaborative research and development.

Approximately 35 participants attended the event from various backgrounds, including cloud providers, academia, government entities, professionals in public health and cybersecurity, and representatives from security vendors and community organizations.

We had two short keynotes on Public Health (Nathan Taback, University of Toronto) and Cyber Public Health (Adam Shostack, University of Washington and CyberGreen). These were followed by two breakout working sessions, one on definitions and one on data, each followed by a readout which allowed us to share insights from the breakout sessions to the larger group. Finally, we held an organizing session in which we asked each person for next steps, then grouped them.

Background: Cyber Public Health as a new approach

There are persistent problems in cybersecurity, and perhaps new perspectives can help us solve them. Preliminary work seems promising.

It is difficult today to characterize the health status of the internet and its connected services, devices, and people. There are no clear and universal definitions for describing the entities we aim to keep healthy – whether they are people, computers, or accounts. There is no consensus on what constitutes their morbidity or mortality. There is no way to measure what specifically confers health benefit, so we cannot tell what interventions lead to good outcomes and avoid bad outcomes. We have no methods to make public internet health decisions – like when to isolate or constrain a small population to preserve the safety of a broader population (e.g. the equivalent of the mandatory quarantine of antibiotic-resistant TB positive humans).

Models in use today often focus too narrowly on the adversary-defender dyad. They fail to look at both the larger context in which the “battle” is unfolding (e.g. are there others also fighting similar adversaries, or is there some collective action we could take that would help us all?), nor

do they help guide preventive actions and behaviors which, when taken, bring benefit to the larger population.

In Cyber Public Health, data is critical. While there is much to be gained by scanning public resources, significant online activity remains under private control. Moreover, many compromises and system failures are not disclosed and so little can be learned collectively about what created vulnerability, how it was exploited and what provided cure and future prevention. To move this field forward, we need the engagement of commercial organizations to help both deepen and broaden datasets to allow us to understand and track Internet health risk factors.

Nearly 30 years ago, the world set out to understand the human genome – to understand the composition of what makes us human and what causes disease. It was a significant computational problem, but one that was able to be solved with a global collaborative effort. The time to make such an effort for global Cyber Public Health is here. With collaboration, data collection, and applying new ways of thinking about cybersecurity, we can build a more resilient Internet.

Guiding questions & key observations

The day had two working sessions: one that focused on definitions and the other which focused on data. We facilitated conversation by providing some guiding questions to breakout groups. We used the Chatham House Rule, so these are both unattributed, and should be read as arguments raised, not agreed. Below, we summarize some key takeaways and discussion points from each session:

Q: What are the units of CPH which should be measured?

- Most groups touched on (at least) some “points of measurement” such as devices, accounts, users, applications, networks, enterprises, and third parties. What properties of these objects would be measured?
- Similarly, there was discussion around targets we want to protect. Where public health focuses on threats to humans, what target(s) should cybersecurity focus on protecting?
- Should we focus on actors who *cause* harm and/or actors who *experience* harm?
- Differentiating factors in ontology may come down to how well defined they are and how well the relationships are mapped relative to one another.
- How can we measure cyber resiliency and recovery investment?
- There are different levels of analysis that could be considered, such as asset or actors, strategic or operational.
- And then a different perspective is looking at this across a timeline:
    - preparedness → response (during event) → recovery (post event)

Q: What are the harms in CPH?

- Impact to “Digital Activities of Daily Living” (ADL) were put forth as a category of harms. Another group chose to list some different types of harms, such as technical harms, breaches, violations of CIA, harms to trust, risk conditions, etc.
- There were some thought-provoking questions pertaining to legal issues and we explored the role of impact in the context of harms.
- Some issues with current systems were brought up, with one example related to CVSS and the breadth of its coverage.
- Some potential next steps and solutions were posed around refining definitions, collecting data, and establishing the institutions to do so.

Q: Cyber Public Health Data sources – what are they, who has access?

- An argument was put forth that “the data is out there, we would just need someone to pay for it.” It’s not clear that this is true, that collection methods are aligned, definitions are clear, etc. but it’s a fascinating and provocative perspective.
- We enumerated some potential data providers and types of data.
- There was extensive discussion around entities that could collect data.
- Unlike professions in medicine, cybersecurity doesn't have a licensing regime that can be used to compel reporting.
- It’s hard to count computers in the world accurately.
- There was discussion of age as a measurement of risk - older devices are more vulnerable. Should we be collecting data related to this? What other risk factors from public health should we consider in Cyber Public Health?
- This led to a more concrete discussion on cost, both financial and reputational.
- There was discussion around potential next steps and solutions which include professionalizing the industry, reducing liability related to reporting, incentivizing good practices, and implementing government regulations.

Next steps

- The most immediate next step is a detailed report, planned for late May 2024. We would love your feedback, advice or leadership in any of the following. Help us identify achievable “wins” that will show the value in the next year.
- Creating a community communication platform (perhaps Slack or Discord)
- Applying for grants, including an NSF “Research Coordination Network”
- Planning for ongoing use of the Ostrom Workshop Cyber Public Health Workshop (seminar series, 4th Thursday of the month at 3pm ET; sign up here)
- Planning for a next event
    - Are there conferences or events that we should attach to/align with?
    - Should we hold another workshop-centered event, or something with a call for papers/reviewing process?
- Collaborating on research and papers
- Add your work to a collaborative bibliography which will be included in the detailed report.