CyberGreen

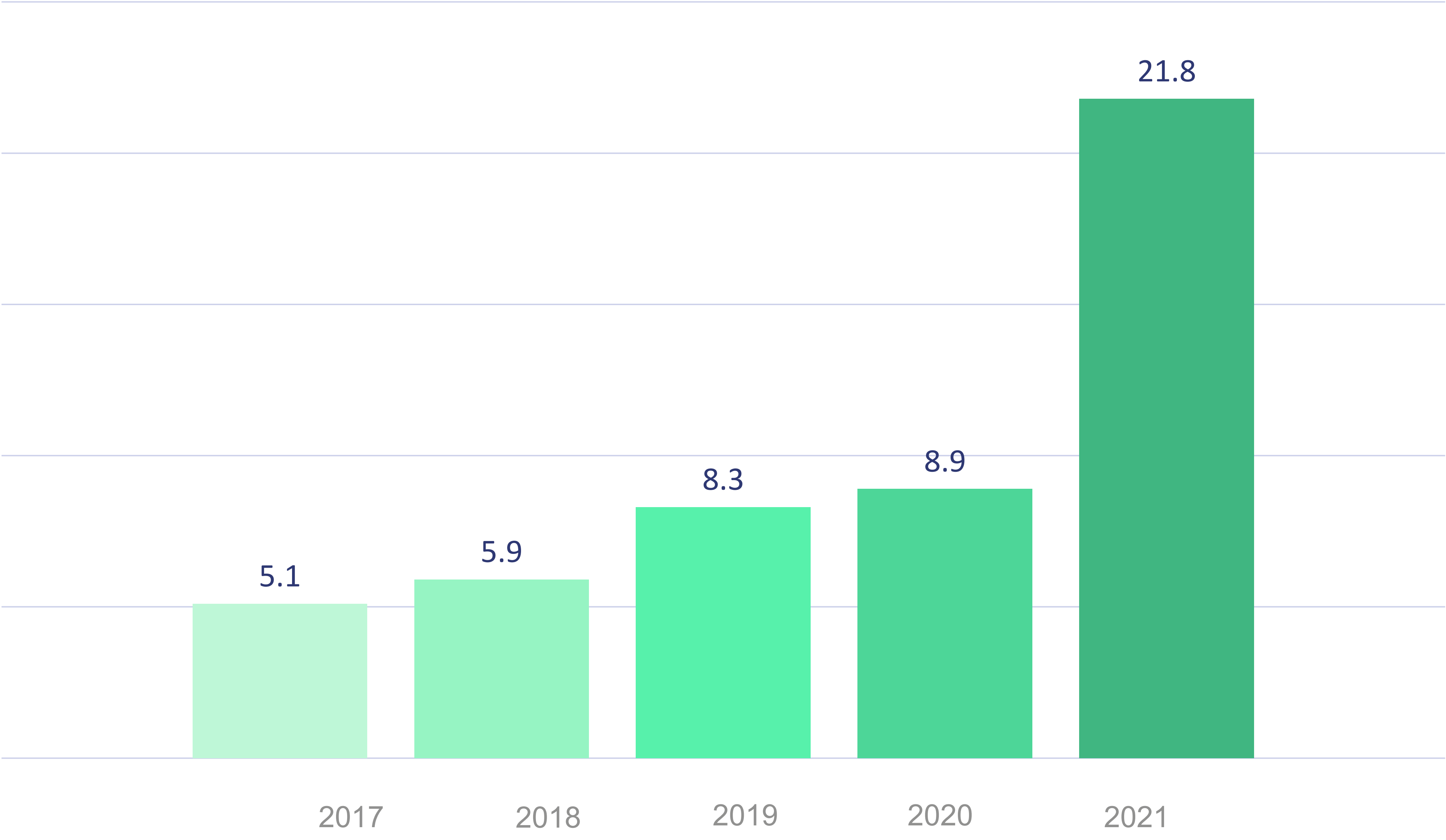
Cyber Belief Model

Workshop hosted by CyberGreen

September 28, 2022

CYBER THREATS & SPENDING SKYROCKETING

GLOBAL VC INVESTMENT UP 400% *



* Data from Crunchbase

GLOBAL CYBERSECURITY SPENDING 2021*

$185

BILLION

* Data from Cybersecurity Ventures

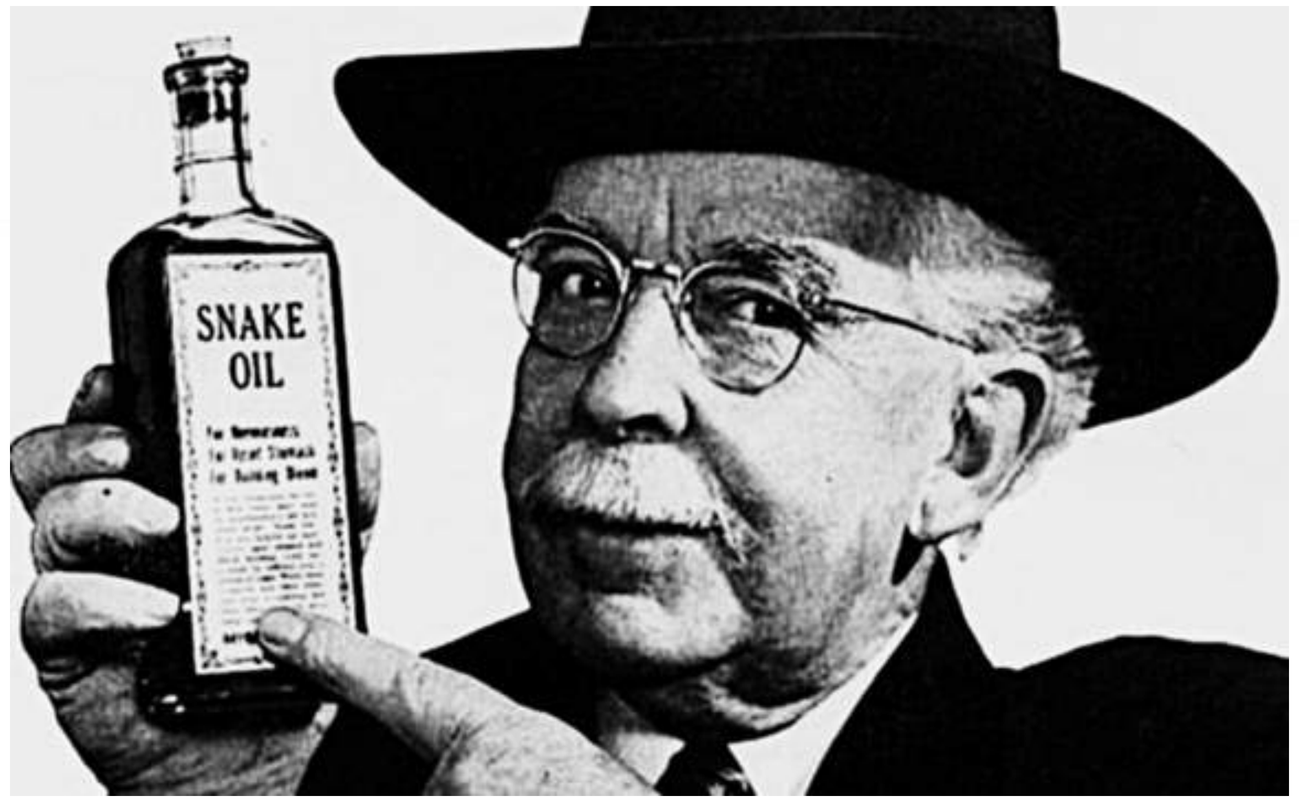
BUT . . . WE DON’T REALLY KNOW WHAT WORKS & WHAT DOESN’T

We are unable to assess the effectiveness of mitigation efforts, identify the wider determinants of cyber security risk, or predict future outcomes.

We do not have vast quantities of robust data for assessment.

DRAWING INSPIRATION FROM THE HISTORY OF MEDICINE

At the dawn of the 19th Century, the practice of medicine faced a similar set of challenges.



GLOBAL PANDEMICS

Deadly outbreaks of infectious diseases including smallpox and cholera increasingly threatened communities around the world, exposing the limitations of existing practices.

SNAKE OIL & SUPERSTITION

The practice of medicine was plagued by false theories of disease and ineffective treatments, but it had no effective means to resolve those questions.

CyberGreen

A NEW PERSPECTIVE

The emergence of Public Health and Epidemiology revolutionized the practice of medicine in the 19th Century. They shifted the perspective and approach in four ways that are particularly relevant to cybersecurity.

Adopting a public health-style perspective that embraces **data-driven investigation**, **population-level analysis**, and **preventative approaches to shared risks** would be transformative for the practice of cybersecurity.

Systematic Testing

Experts could systematically test associations between risk factors and cyber threats

Measure and Compare

Cybersecurity professionals could truly measure and compare the effectiveness of interventions.

Preemptively Address Risk

Organizations and companies could adopt preventative measures that reduce both local and systemic risks to make the internet more secure and resilient for all.

More Effective Enterprise Security

The data and analytical techniques developed through Cyber Public Health research will enable enterprise security teams to better evaluate existing practices, test alternatives, and better predict future threats.

CyberGreen

BRING DATA & METRICS TO CYBERSECURITY DECISION-MAKING

ECOSYSTEM-WIDE BENEFITS

From app developers to government officials to cybersecurity professionals, access to more comprehensive data and metrics would enable better decision-making, more efficient use of resources, and more secure systems.

CyberGreen

CyberGreen’s mission is to establish a science of Cyber Public Health dedicated to making the internet safer and more resilient for all.

TIMELINE

YEAR 1

DATA, METRICS & SCORING

Begin measuring and scoring global cyber risk and public health at the national level.

FOUNDATIONAL RESEARCH

Research mitigation practices and barriers to adoption, and partner with policymakers and network operators on risk reduction study.

ADVOCATE FOR NEW DATA

Advocate for expanded data collection to support public health approach with policymakers and other stakeholders.

YEAR 5

CAPACITY BUILDING

Two regional Cyber Public Health Centers established and a capacity building program at National Cyber Census Office.

ADVANCING CPH SCIENCE

Establish Cyber Public Health within professional and academic communities with sessions at key conferences and governance forums.

NATIONAL SCORING SERVICE

Offer CPH scoring at the national level as a paid service.

YEAR 10

CPH IN ACADEMIA

Introduction of graduate level Cyber Public Health courses at 1-2 colleges.

CPH BOOK

Publication of first book dedicated to the science of Cyber Public Health.

GOVERNMENT CPH INCENTIVES

National regulations that promote collection and sharing of critical CPH data and mitigation efforts designed to minimize collective risk..

CyberGreen

METRICS & MEASUREMENT

What we collect and measure

TODAY

01 Weekly global scans for open services (DNS, NTP, SNMP, SSDP, CHARGEN).

02 Approximately 4 billion IPv4 addresses scanned globally and cross referenced with every country and over 100,000 Autonomous Systems Numbers (ASNs).

SCALING UP (2022-2023)

01 Development of a comprehensive framework with 6 components, including open services.

02 Research and development for a prototype system that measures the public health of open services, routing security, and DNS.

03 Currently testing routing security by ingesting third party data related to RPKI and cross referencing it with geolocation data (country and ASN levels).

04 Finalization and expansion of the prototype to automate data ingestion, metrics, calculations, and scoring of all components (addition of email security, certificates, and security protocols & services).

CyberGreen

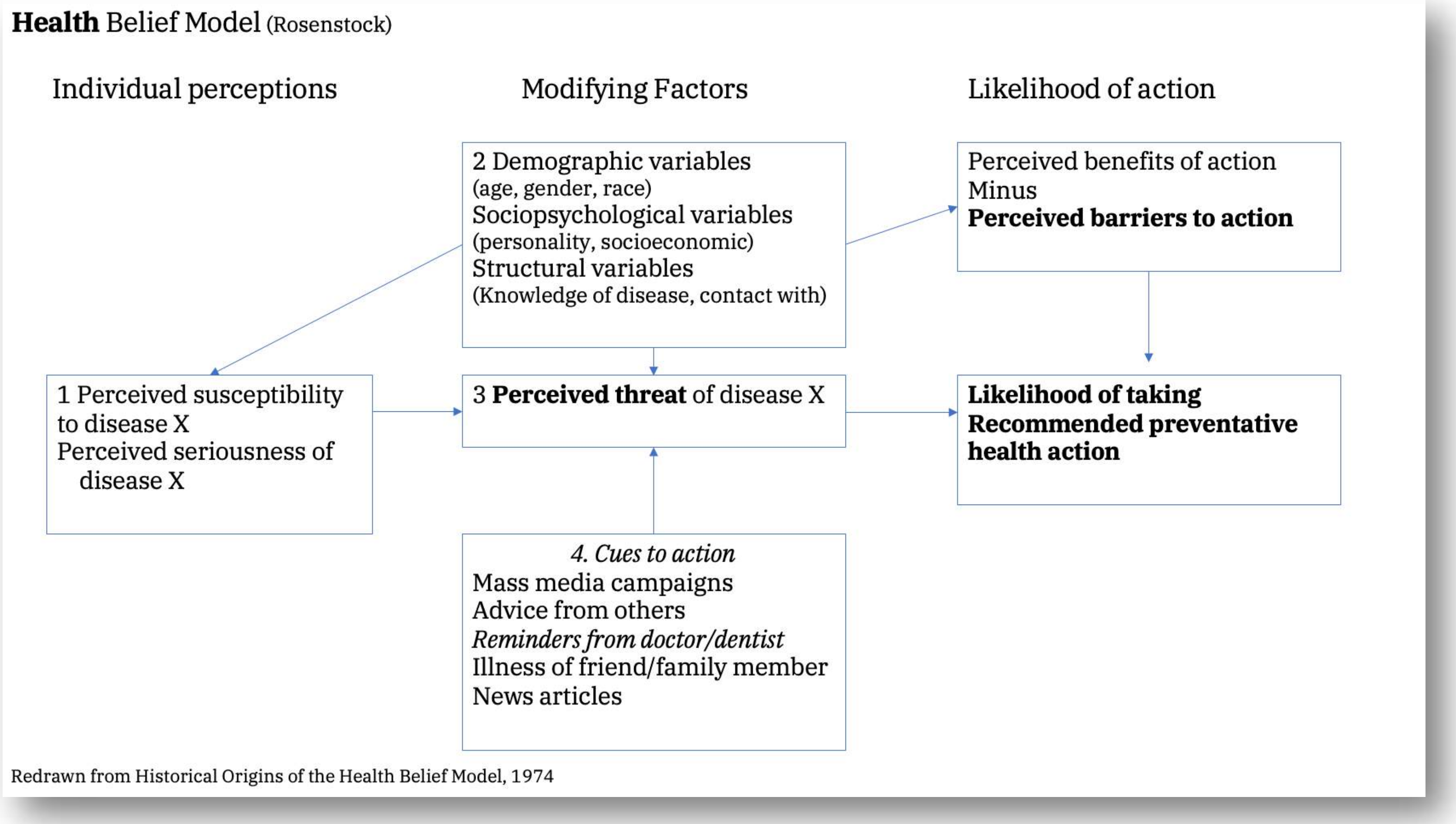
Project background

Why don’t they just…

This question applies to cyber defenses, such as MFA or DNSSec

CyberGreen

Health Belief Model



Health Belief Model (Rosenstock)

Individual perceptions

Modifying Factors

Likelihood of action

2 Demographic variables
(age, gender, race)
Sociopsychological variables
(personality, socioeconomic)
Structural variables
(Knowledge of disease, contact with)

Perceived benefits of action
Minus
Perceived barriers to action

1 Perceived susceptibility to disease X
Perceived seriousness of disease X

3 **Perceived threat** of disease X

Likelihood of taking Recommended preventative health action

4. Cues to action
Mass media campaigns
Advice from others
Reminders from doctor/dentist
Illness of friend/family member
News articles

Redrawn from Historical Origins of the Health Belief Model, 1974

BELIEFS INFLUENCE ACTIONS

Well established truth in public health

A SET OF MODELS

Cues to action

Demographics

Perception of threat

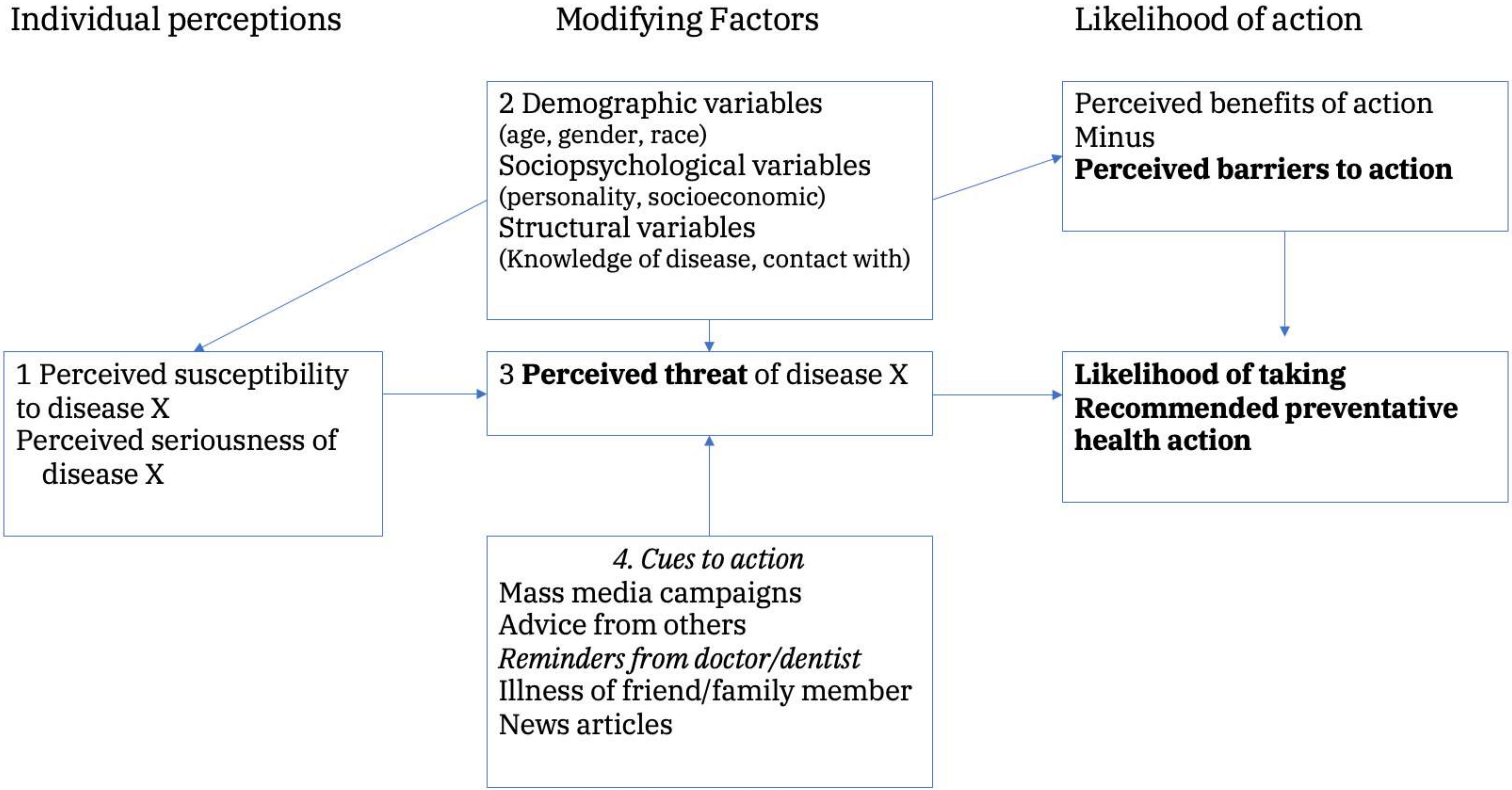
Perceived costs and benefits

ANALYTIC FRAMEWORK?

Can we adapt this model to cybersecurity?

Does it teach us useful things?

Health Belief Model (Rosenstock)



Individual perceptions

Modifying Factors

Likelihood of action

2 Demographic variables
(age, gender, race)
Sociopsychological variables
(personality, socioeconomic)
Structural variables
(Knowledge of disease, contact with)

Perceived benefits of action
Minus
Perceived barriers to action

1 Perceived susceptibility to disease X
Perceived seriousness of disease X

3 **Perceived threat** of disease X

Likelihood of taking Recommended preventative health action

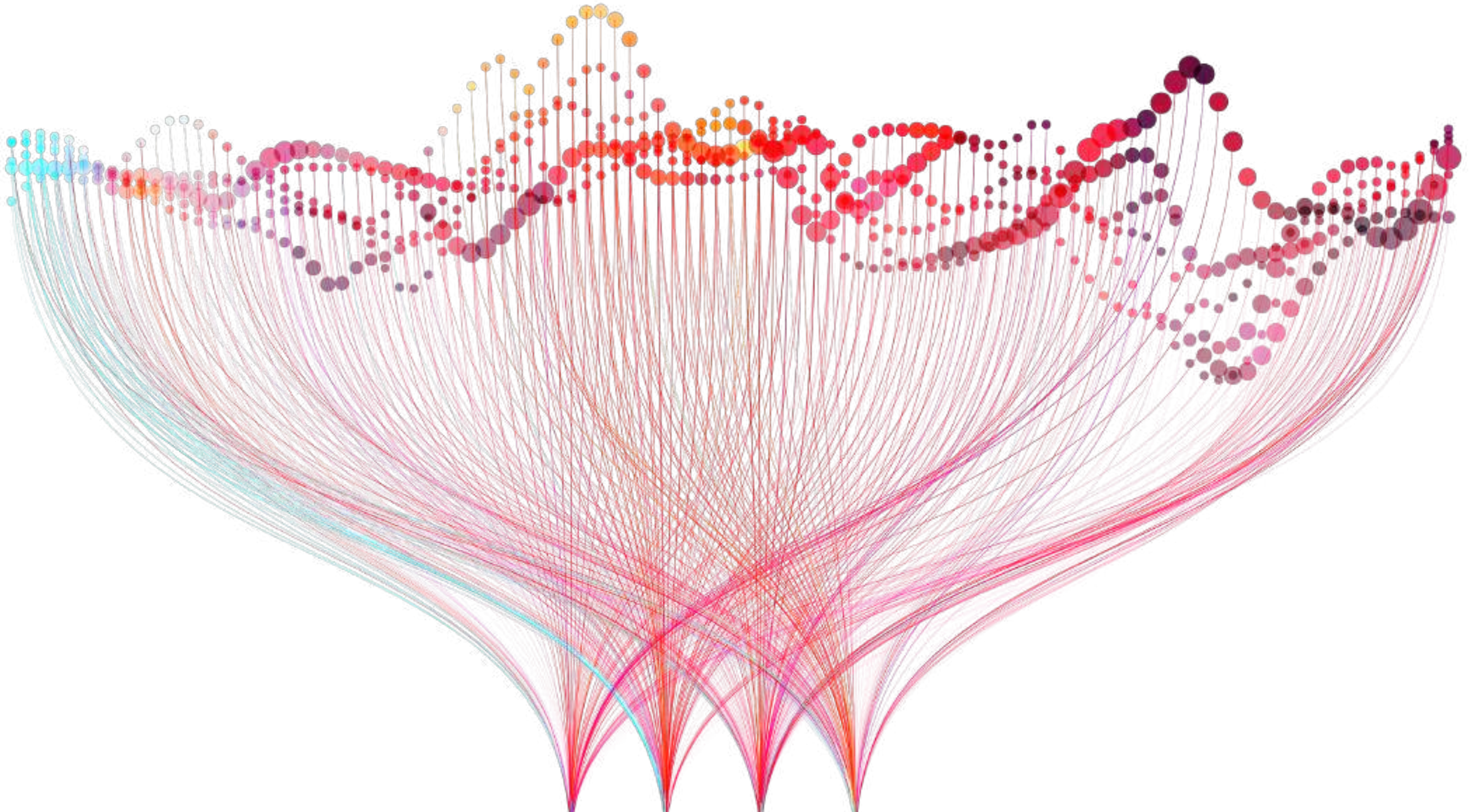
4. Cues to action
Mass media campaigns
Advice from others
Reminders from doctor/dentist
Illness of friend/family member
News articles

Redrawn from Historical Origins of the Health Belief Model, 1974

TikTok?

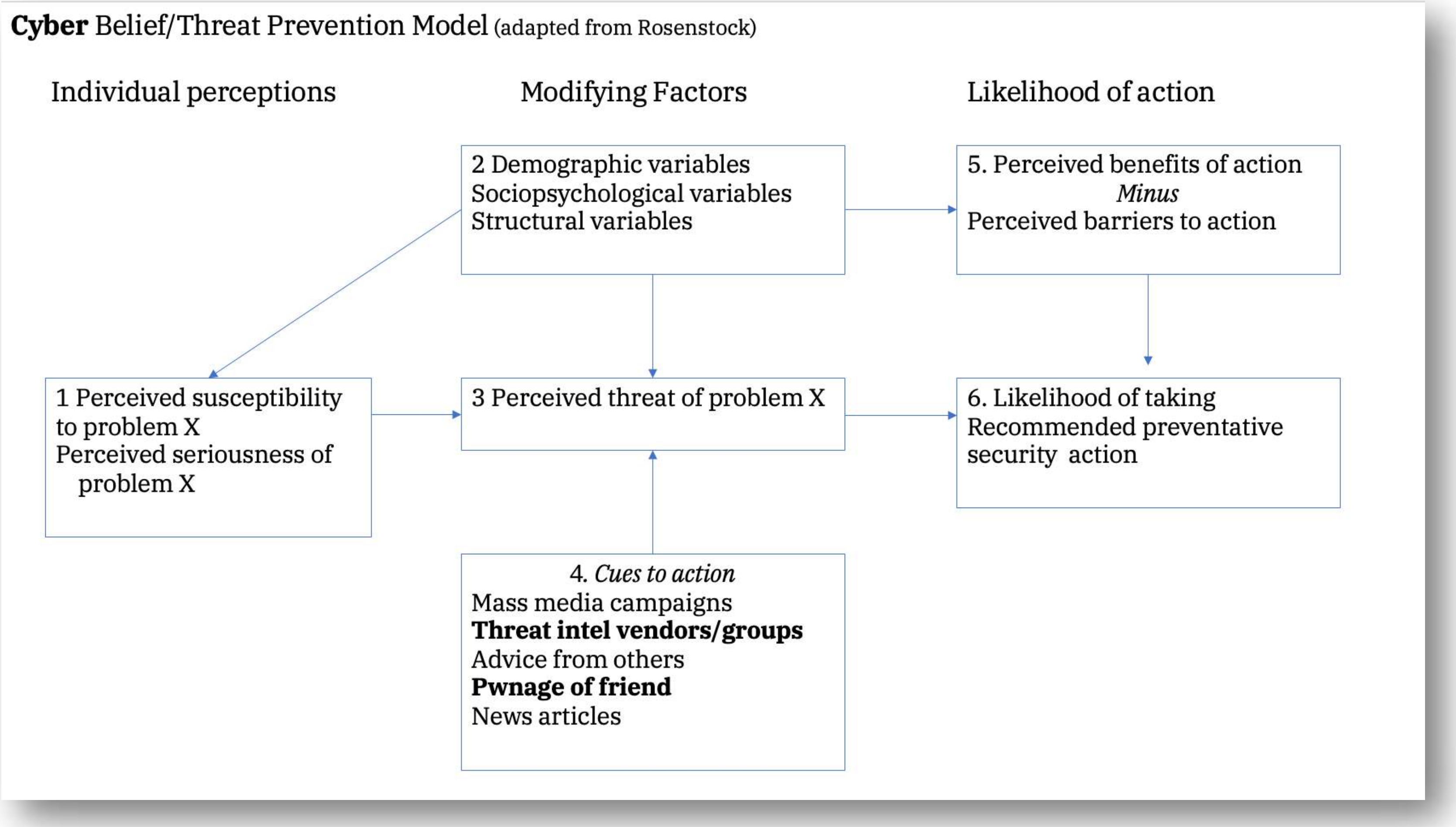
- Vague descriptions of threats
- Many threatening apps?
- Clear costs of “delete the app”

Understanding
risky behavior may
help us influence it



CyberGreen

Cyber Belief Model



Cyber Belief/Threat Prevention Model (adapted from Rosenstock)

Individual perceptions

Modifying Factors

Likelihood of action

2 Demographic variables
Sociopsychological variables
Structural variables

5. Perceived benefits of action
Minus
Perceived barriers to action

1 Perceived susceptibility to problem X
Perceived seriousness of problem X

3 Perceived threat of problem X

6. Likelihood of taking Recommended preventative security action

4. *Cues to action*
Mass media campaigns
Threat intel vendors/groups
Advice from others
Pwnage of friend
News articles

BELIEFS INFLUENCE ACTIONS

Well established truth in public health

A SET OF MODELS

Cues to action

Demographics

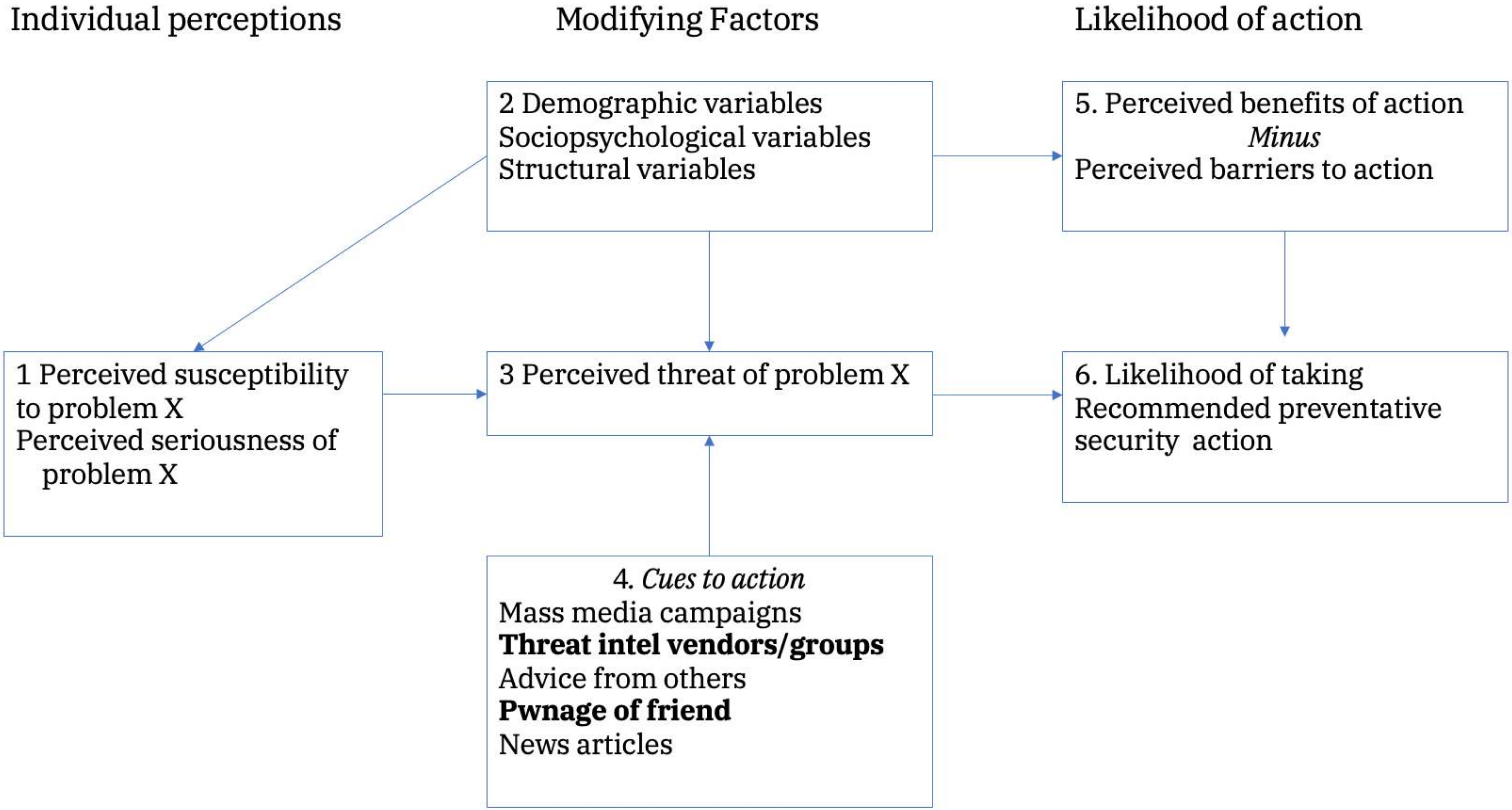
Perception of threat

Perceived costs and benefits

Let’s test it

What happens if we apply this to real problems?

Cyber Belief/Threat Prevention Model (adapted from Rosenstock)



Individual perceptions

Modifying Factors

Likelihood of action

2 Demographic variables
Sociopsychological variables
Structural variables

5. Perceived benefits of action
Minus
Perceived barriers to action

1 Perceived susceptibility to problem X
Perceived seriousness of problem X

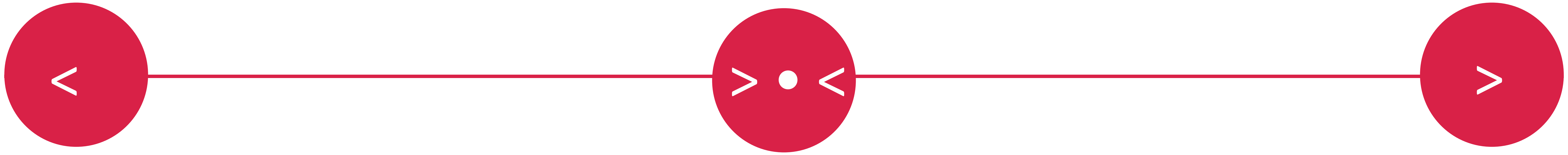
3 Perceived threat of problem X

6. Likelihood of taking
Recommended preventative security action

4. *Cues to action*
Mass media campaigns
Threat intel vendors/groups
Advice from others
Pwnage of friend
News articles

The project + preliminary results

TIMELINE



Interviews

7 CISO Types
45-60 minutes in August
Recorded

Analysis

Coded interviews
Learned about recruiting + scheduling

Preliminary results

Model created
Coding system created, refined
Seems illustrative, explanatory

Return on investment?

"Cues to action" seem saturated
May need attention:

- Barriers
- Assessing susceptibility

Sharing + Listening

What do you think
Where should we go?

Tech report forthcoming

Subscribe at cybergreen.net

What we’ve done so far

CyberGreen

- Created a preliminary model
  - Refined as we interviewed
- Recruited and interviewed participants
  - 7 senior security managers/execs
  - Tech providers + tech consumers
  - Modern scientific practice (explain; skip or leave)
  - Semi-structured (14 core questions)
- Recorded calls, transcribed and then “coded”
  - Created and evolved as we went

First impressions

- Getting interesting results (next slides)
  - All analysis is in progress, results may change
- Low takeup on “is there anything else” questions
- Interviewees were
  - Shown current draft
  - Invited to challenge

Results 1/3: Many cues to action

- Cues include:
  - Twitter
  - Threat intel feeds, groups
  - CISA
- Cues carry challenges
  - Hard to distinguish
  - Hard to track who’d seen what

Results 2/3: Many barriers to action

CyberGreen

- Barriers included:
  - Lack of system inventory, shallow inventories
    - SBOM?
    - At least one participant asserted SBOM wouldn’t have helped
    - (Knowing what’s deployed globally is hard, never mind getting SBOMs)
  - Holiday season
  - Stream of issues
  - Norm of only fixing internet-facing issues

Results 3/3: Susceptibility questions

- “But it’s not internet facing!”
- Avalanche of requests to + from vendors
  - Data
  - Attestation
- Requests were dis-similar
  - Log4Shell? CVE-2021-44228?
  - Delay for completeness/correctness versus immediacy

Meta-result: Barrier to action

- Many spontaneous comments about the cost
- Log4shell may have exhausted resilience and preparedness

The path ahead

Today: sharing preliminary results

CyberGreen

- What do you think?
- Seeking thoughtful feedback
- Via
  - here today
  - @adamshostack or @cybergreen on linkedin
  - Email contact@cybergreen.net

Please explore

CyberGreen

- This is a research tool today
- Try the CBM as a rubric for stalled initiatives
- We’re happy to share code list + guidance

Later this year

- Releasing tech report on cybergreen.net

CyberGreen

ESTABLISH A SCIENCE OF CYBER PUBLIC HEALTH

DATA & METRICS

Science starts with data, so our top priority is gathering a more comprehensive set of data and standardizing it for researchers.

SOCIETY-LEVEL VIEW

A society-level view of risks will revolutionize every aspect of cybersecurity, including reducing systemic risks, addressing existing inequities, and making the internet more secure and resilient for all.

INSTITUTIONS & INFRASTRUCTURE

We need institutions at every level of government, international NGOs, academic institutions, and private organizations to support a mature science of Cyber Public Health.

Thank you!

Interview prompt list

1. What was your role in handling log4shell and related vulnerabilities?
2. How did you personally first become aware of one of the issues?
3. How did you perceive its seriousness?
    a. why did you think this?
    b. how did you quantify or rank that?
4. How did you think about susceptibility?
5. if personal awareness proceeded formal organizational plans:
    * Did you work to make others aware of the issue?
    * Were there things they brought up that made it harder to take action?
6. If organizational awareness proceeded personal awareness
    * how did you become aware?
    * what was your role?
7. Did you set up a formal approach to hearing about variants?
8. Were you aware of any question from leadership about the benefit of the work? (if so, what?)

8a. disagreement on approach or reasons that it was hard

9 - what's confidence that your work improved your security or that of your customers?

10. are there things you did that didn't seem effective? (Don't fail to followup + probe)
11. what, if anything, are you doing differently as a result of your experience?
12. After log4shell is your belief in your ability to protect your systems improved/neutral/diminished?
13. What else comes to mind about the issue?
14. Are there things that fit/don't fit/contradict the model?
15. what else should I ask?