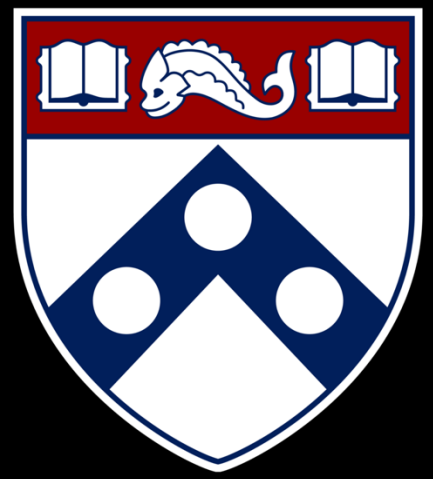
Empirical Security & Privacy, for Humans

UPenn CIS 7000-010

11/06/2025



Lessons for Cybersecurity from the American Public Health System

Readings

September 2016

March 2025

Input to the Commission on Enhancing National Cybersecurity

Steven M. Bellovin
https://www.cs.columbia.edu/~smb
Columbia University[1]

Adam Shostack
http://adam.shostack.org
Independent

Thank you for the opportunuty to provide Input to the Commission on Enhancing National Cybersecurity. This is a joint submission by Steven M. Bellovin and Adam Shostack. Steven M. Bellovin, a member of the National Academy of Engineering, is the Percy K. and Vida L.W. Hudson Professor of Computer Science at Columbia University. Adam Shostack is an entreprenuer and the author of *Threat Modeling: Desinging for Security*.

We are writing after 25 years of calls for a "NTSB for Security" have failed to result in action. As early as 1991, a National Reseach Council report called for "build[ing] a repository of incident data" and said "one possible model for data collection is the incident reporting system administered by the National Transportation Safety Board." [1] The calls for more data about incidents have continued, including by us [2, 3].

The lack of a repository of incident data impacts our ability to answer or assess many of your questions, and our key recommendation is that the failure to establish such a repository is, in and of itself, worthy of study. There are many factors in the realm of folklore as to why we do not have a repository, but no rigorous answer. Thus, our answer to your question 4 ("What can or should be done now or within the next 1-2 years to better address the challenges?") is to study what factors have inhibited the creation of a repository of incident data, and our answer to question 5 ("what should be done over a decade?") is to establish one. Commercial air travel is so incredibly safe today precisely because of decades of accident investigations, investigations that have helped plane manfacturers, airlines, and pilots learn from previous failures.

The problem, in its simplest form, is that we do not have a good idea of what is going wrong in cyber-security. Lacking a repository of incidents, information about the causes of those incidents, or means of discussing controls, we are unable to assess scientifically if our advice is effective. (To your question 1, why is asking the public what are current trends and challenges the core of deciding a research agenda? Why do we not have a more structured way to learn that?)

We lack a repository because we have tacitly agreed that having such a repository is not worth overcoming the barriers to its creation, and we have tacitly agreed to not discuss our mistakes. The reasons for this are worthy of study, and such study should inform efforts to overcome our inability to learn from our mistakes. A better understanding of

2024-2025 CRA Quadrennial Paper

Lessons for Cybersecurity from the American Public Health System

Adam Shostack (University of Washington), L. Jean Camp (Indiana University), Yi Ting Chua (University of Tulsa), Josiah Dykstra (Trail of Bits), Brian LaMacchia (FARCASTER Consulting Group), Daniel Lopresti (Lehigh University)

> **The United States needs national institutions and frameworks to systematically collect cybersecurity data, measure outcomes, and coordinate responses across government and private sectors, similar to how public health systems track and address disease outbreaks.**

Public Health and Cybersecurity Public Health

Public health is a discipline focused on the health of populations. Public health and medicine complement each other, and their advances lead to measurable extensions of human life, such as nearly doubling population life expectancy during the 20th century. Public health allows for the comparison of alternative courses of treatment for best effectiveness and enables the allocation of limited resources to have the greatest possible impact on the largest at-risk population.

The advantage of taking a public health approach to disease is exemplified by one of its earliest examples. In 1854, while England — and particularly London — was suffering through an epidemic of cholera, physician John Snow theorized that the disease spread via water rather than air, as was assumed. To test his theory, Snow took a novel approach of mapping the locations of cholera deaths in the city and city water pumps. He noticed that deaths appeared to be disproportionately clustered around a particular water pump on Broad Street. When he removed the pump handle,incidences of cholera dropped considerably. Snow also performed a statistical analysis of cholera deaths among customers of two different water companies drawing from different parts of the Thames River — one that drew close to the city and one that drew further upstream, and therefore likely less polluted from city sewage. The population served by the upstream water company had 14 times fewer cholera deaths, further strengthening his hypothesis. It was a convincing demonstration of the value of a public health approach, combining medical knowledge and data with spatial and statistical data to point to an effective course of action.

September 2016

Commission on Enhancing National Cybersecurity

The Commission will make detailed **recommendations** to **strengthen cybersecurity** in both the public and private sectors while protecting privacy, ensuring public safety and economic and national security, **fostering discovery and development** of new technical solutions, and **bolstering partnerships** between Federal, state, and local **government and the private sector** in the development, promotion, and use of cybersecurity technologies, policies, and best practices.

https://en.wikipedia.org/wiki/Commission_on_Enhancing_National_Cybersecurity

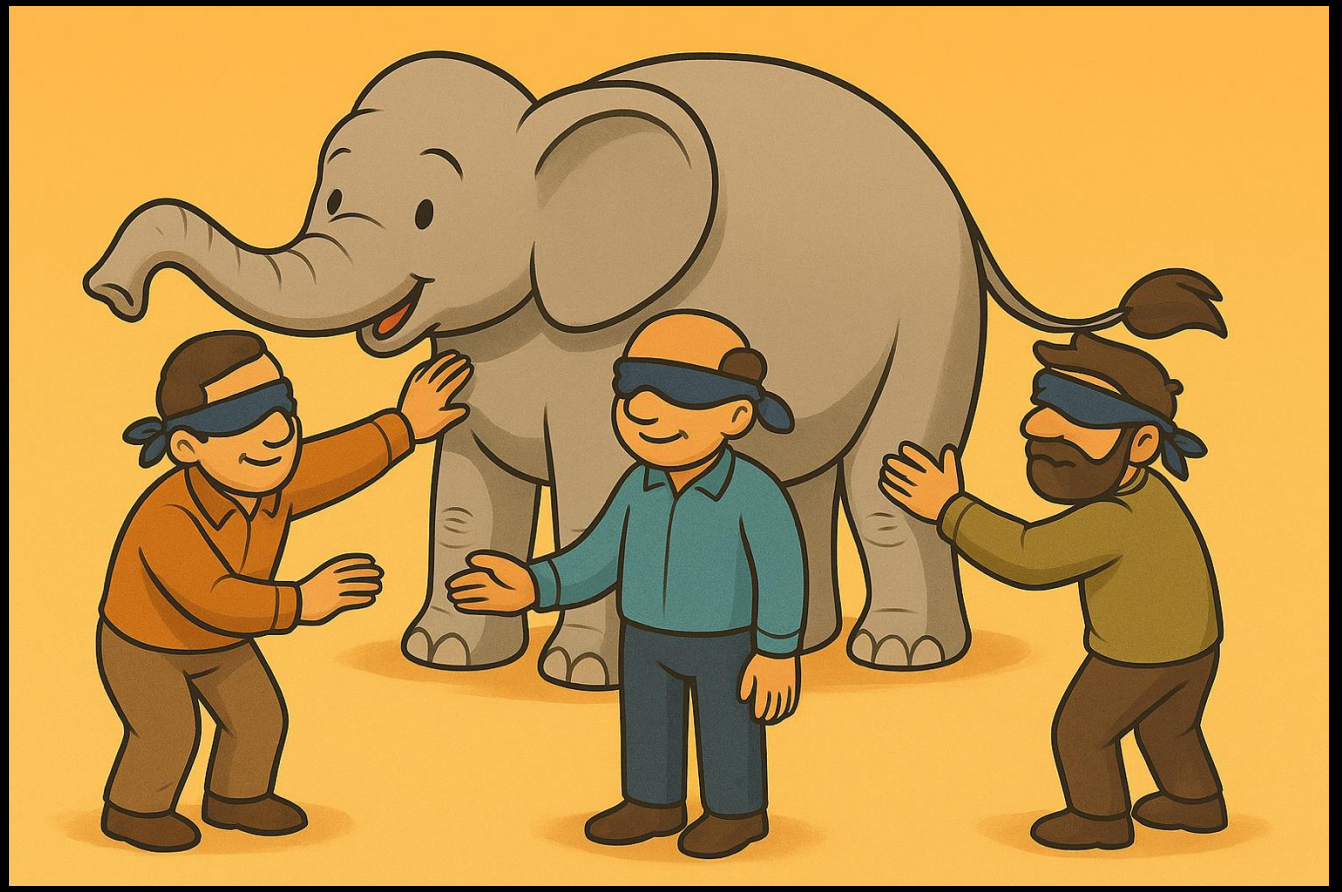
How do you know you are “enhancing” ?

Bellovin & Shostack:

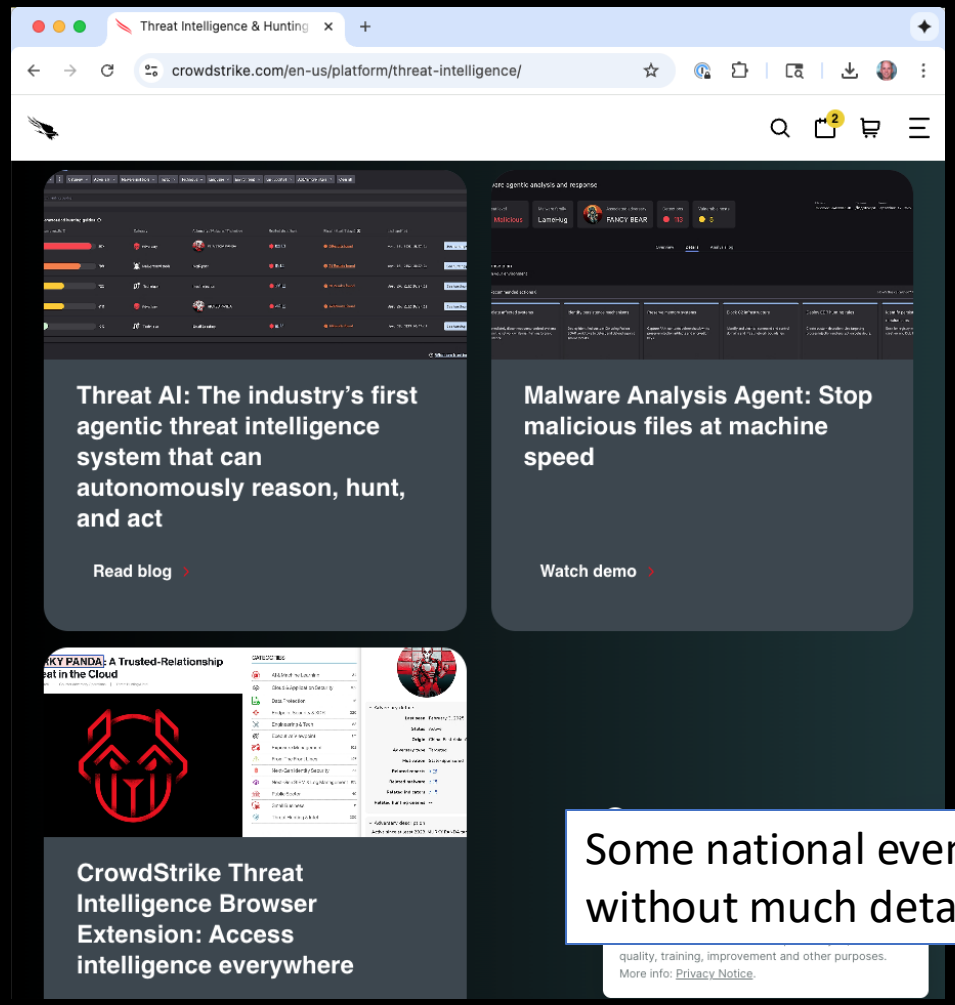
“Lacking a repository of incidents, information about the causes of those incidents, or means of discussing controls, we are unable to assess scientifically if our advice [on improving cybersecurity] is effective.”

Comparison:
Safety improvements in air travel are, in part, due to careful analysis of failures

Org data presents an incomplete picture

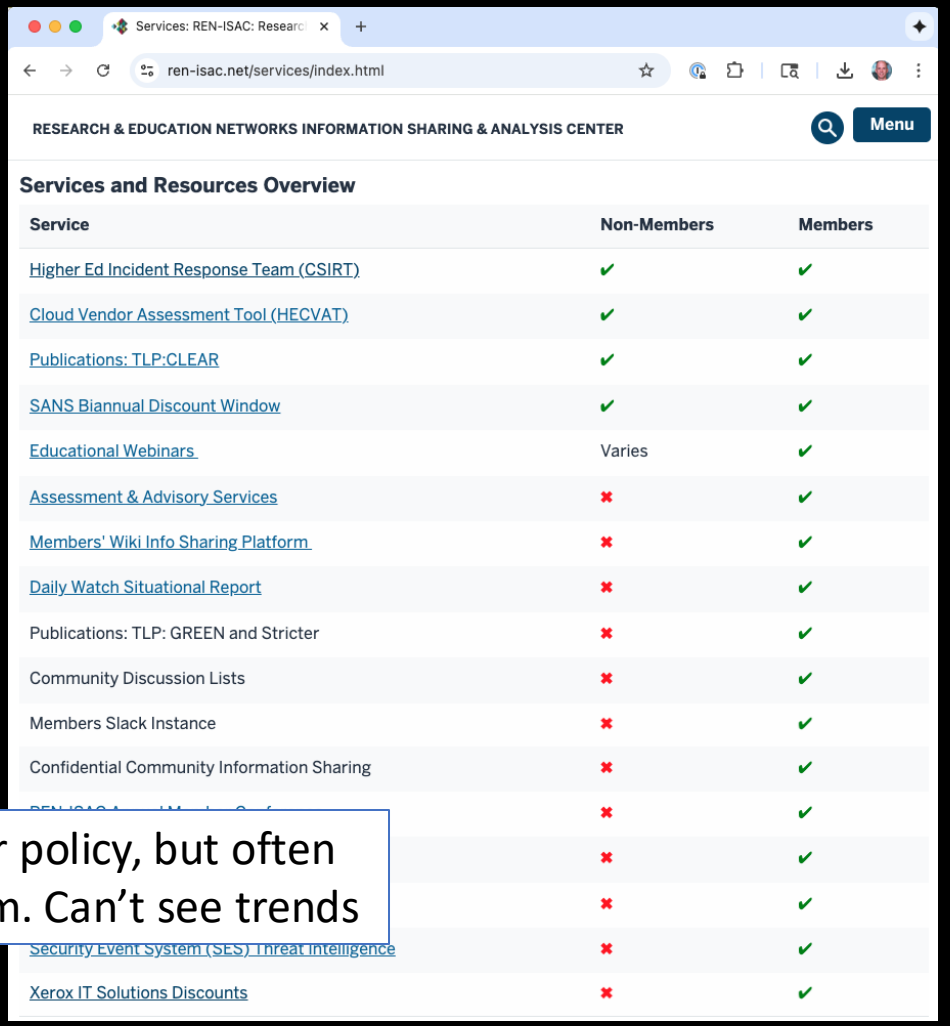


Today: Collecting data within communities



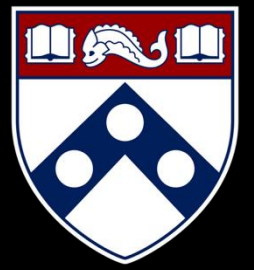
Threat intelligence aggregated from on-premise monitoring capabilities (e.g., Crowdstrike)

Consortia organized for information sharing and improvement (e.g., REN-ISAC)



Some national events publicized, due to law or policy, but often without much detail. So: Can't learn from them. Can't see trends

Outside org/comm: Q but no A



breach of 10/31:

- Did the attacker use a vulnerability or convince someone to take action? ✓ "social engineering" of well-placed account holder
- What controls were in place which might be expected to prevent the attack? ?
- Was there a failure to act on information because of too many alarms? ?
- A mis-configuration? ?
- Did some control simply fail? ?

Some national events publicized, due to law or policy, but often without much detail. So: Can't learn from them. Can't see trends

CWE-656: Reliance on Security Through Obscurity

Weakness ID: 656
Vulnerability Mapping: ALLOWED (with careful review of mapping notes)
Abstraction: Class

View customized information: Conceptual | Operational | Mapping Friendly | **Complete** | Custom

Description

The product uses a protection mechanism whose strength depends heavily on its obscurity, such that knowledge of its algorithms or key data is sufficient to defeat the mechanism.

Extended Description

This reliance on "security through obscurity" can produce resultant weaknesses if an attacker is able to reverse engineer the inner workings of the mechanism. Note that obscurity can be one small part of defense i depth, since it can create more work for an attacker; however, it is a significant risk if used as the primary means of protection.

Alternate Terms

Never Assuming your secrets are safe

Common Consequences

Impact	Details
Other	**Scope: Confidentiality, Integrity, Availability, Other** The security mechanism can be bypassed easily.

A national incident database

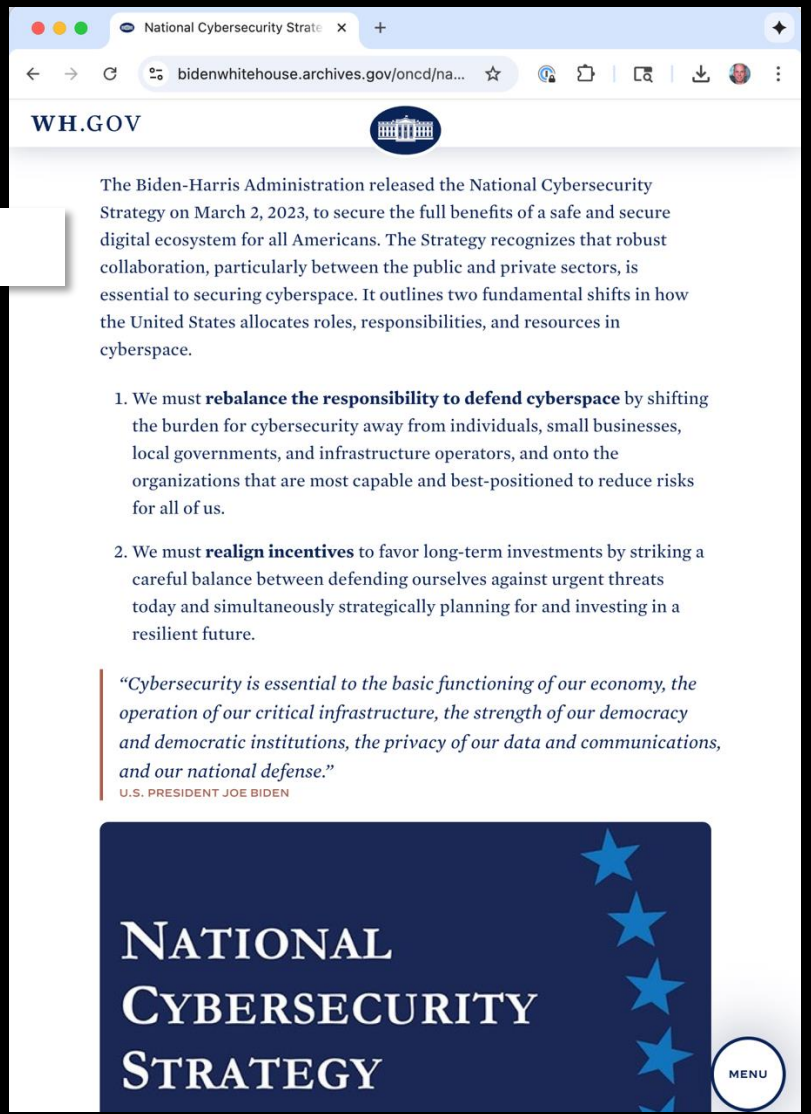
- In general, we want to know “what has gone wrong recently” and “how is that changing?”
- Can then
  - Assess expert advice (SANS top 20 vs. Australian DSD top 35?)
  - Cyber-insurance companies could use it to help set rates, and regulators can mandate (and assess) best practices

How can we get there?

- We have tacitly agreed to not discuss our mistakes. Why?
- In the short term:
  - Anonymous reporting system, like NASA's Aviation Safety Reporting System https://asrs.arc.nasa.gov/ and for railways https://c3rs.arc.nasa.gov/
  - Or: System used by the government for its own lapses. Similar to the intent of the Privacy Act of 1974
- Longer term:
  - Should there a body chartered and funded to gather information about cyber-security incidents?
  - Would research into what methods for analyzing incident root causes generates the best results (and what metrics should be used for assessing best)?
  - What are the tradeoffs between aggregated, anonymized or other approaches to sharing information?

National cybersecurity utterances, since

June 2023



June 2025

September 2025

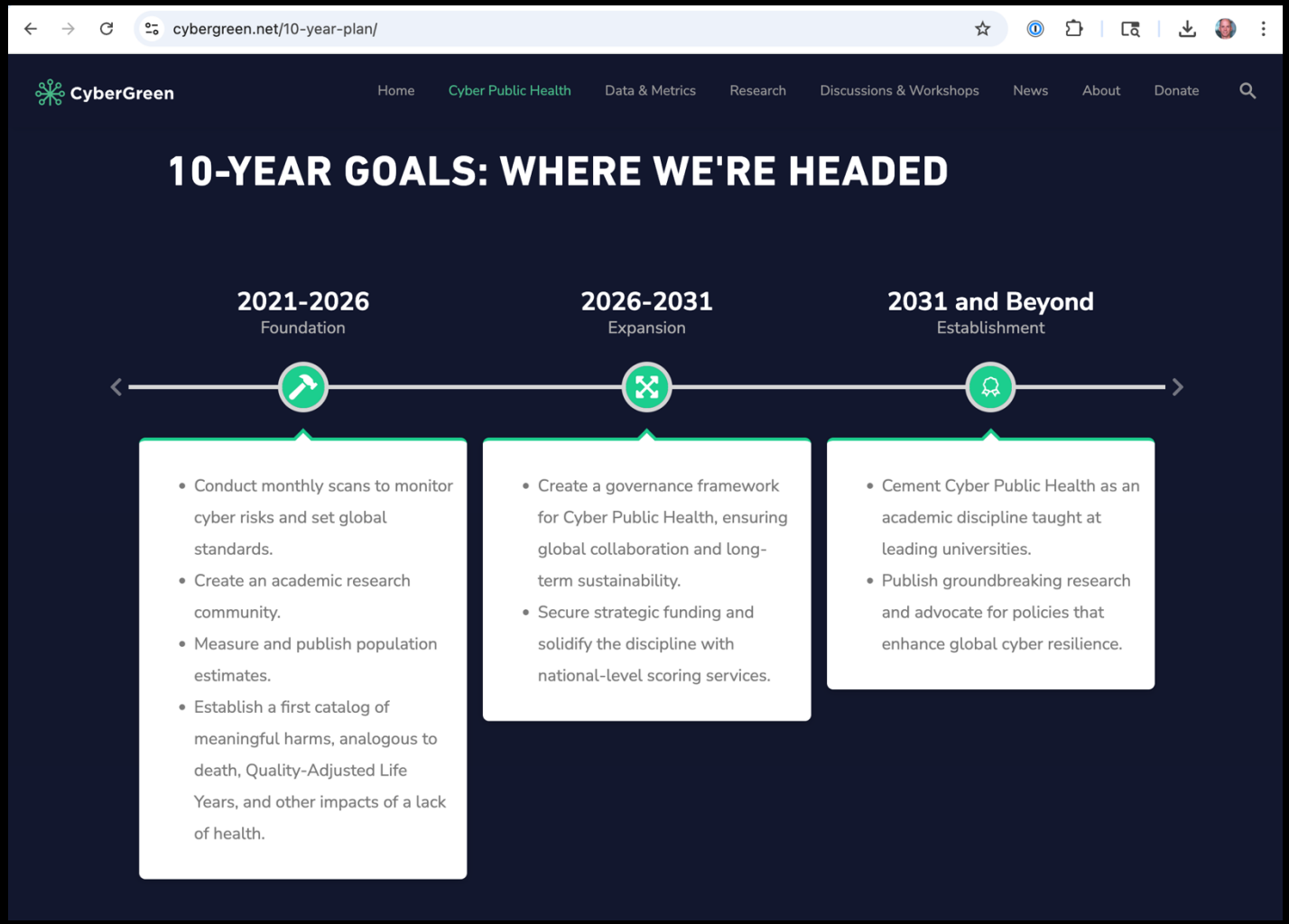
Cairncross said the private sector should have to meet minimum standards for cybersecurity.

Which things should be standard? How do we know they work at scale?

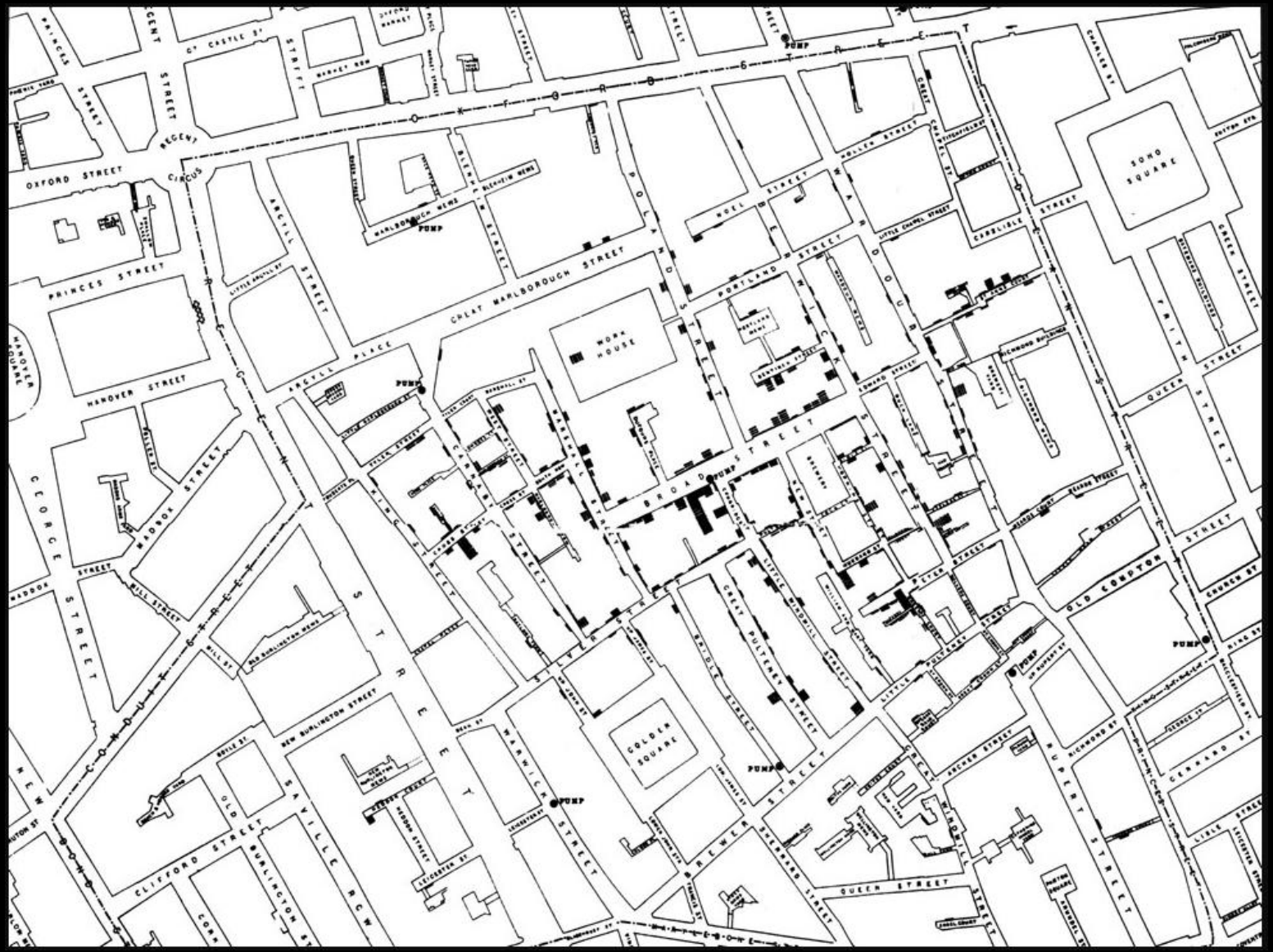
Cyber public health

According to the CDC Foundation, “Public health is the science of protecting and improving the health of people and their communities. … Overall, public health is concerned with protecting the health of entire populations.”

Classic models of cybersecurity have focused on outcomes for the individual or a firm, and the work we’re doing to create a science and discipline of Cyber Public Health aims to **use tools inspired by public health** to bring those **population level measurements** and **improvements** to the cyber realm.



John Snow: Cholera outbreak in 1854

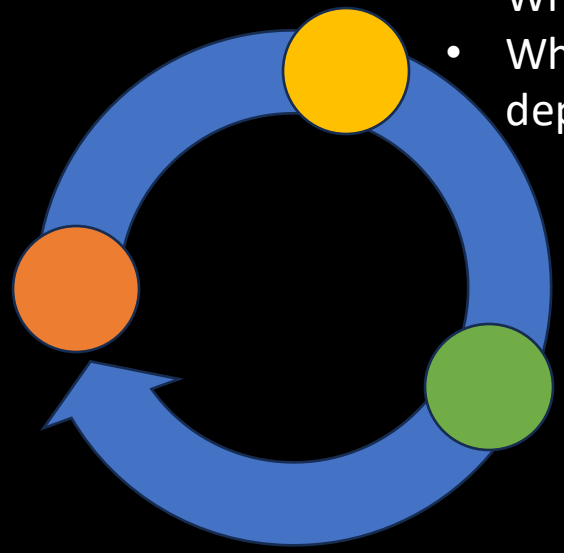


Medicine: How disease works, and how it can be treated on individuals

Public health: Understanding disease risks and treatments at population level, to maximize benefits

Cyber public health in action

Outcomes
- Data breaches,
- Vulnerabilities exploited,
- Financial losses,
- Humans harmed,
- …



Analysis
- What are the (still) successful vectors of attack?
- Where is risk (still) greatest?
- What interventions could be deployed cost-effectively?

Intervention
- Engineering,
- Operations,
- Policy,
- Education, …

What we should see:
- A decline in successful attacks, according to a consistent data collection system
- Updated standards to remove demonstrably ineffective techniques, like password rotation

Proposals for the Fed. Government's role

- Bureau of Cyber Public Health Statistics
- Enable the government to measure and improve cyber controls
  - Focus on whole-of-government efforts
  - Focus on institutions and data
    - Create a National Cybersecurity Data Repository
    - Implement Cybersecurity Health Reporting Standards
    - Incorporate Long-Term Learning
  - Focus on Research
    - Develop Stress Tests for Cybersecurity Public Health in Critical Infrastructure
  - Focus on Creating Community and Collaboration
    - Create Incentives for Private Sector Participation