Title

Adapting a Publicly Focused Individual Health-Care Model to Cybersecurity

Journal

IEEE Security & Privacy, 22(6)

ISSN

1540-7993

Author

Peisert, Sean

Publication Date

2024

DOI

10.1109/msec.2024.3467890

Peer reviewed

Adapting a Publicly-Focused Individual Health Care Model to Cybersecurity

Sean Peisert

September 26, 2024

Sometimes, we all need a little help from our friends — many of us, and especially businesses of various kinds know doctors, lawyers, accountants, building contractors, mortgage brokers, and real estate agents that we can turn to for our needs in the areas of expertise of those individuals. But how many organizations outside Fortune 500 companies in need of computer security expertise know *qualified* professionals that they can turn to? And even if such professionals could be identified, how would one gauge their level of expertise or effectiveness? Unlike every other professional domain mentioned above, there is no state or national computer security licensing board that tracks complaints or disciplinary actions against computer professionals. Indeed, there is limited professional licensing in computer security, so there *are* no disciplinary actions against computer professionals guilty of negligence.

Public health is "The science and art of preventing disease, prolonging life, and promoting health through the organized efforts and informed choices of society, organizations, public and private communities, and individuals." [1] Public health studies a variety of indicators of the health of societies. The methods it uses to effect change are typically sweeping such as national public communication programs to address smoking, promotion of vaccinations during a pandemic or flu season, ensuring clean water, regulations about the addition of iodine or fluoride to table salt, etc.... *Population health* or *community health* extend this notion to vulnerable subpopulations, either geographic, ethnic, or otherwise.

Writing in *The New Yorker* [2] in 2021, Atul Gawande discussed the success of a public health program created in Costa Rica by a Álvaro Salas Chaves, a physician, with the support of the Costa Rican Ministry of Health. Salas's program stands in stark contrast to other countries that spend substantially more on medical care delivery than Costa Rica does, with much lower success, by virtually any measure.

Gawande's piece also notes the limits of traditional public health methods in improving public health. What Gwande discovered is that a combination of traditional public health methods and individual health care was substantially more effective at improving overall public health. To be clear, Costa Rica's approach to the integration of individual health care for public health benefit is not the traditional approach to individual health care used in the United States and other, similarly wealthy nations by providing individual care primarily only to those who can afford it. This approach is individual health care that is "braided" with and closely aligned with public health. As Gawande describes, every Costa Rican has an individual, local, primary health care team, including a physician, a nurse, and trained community health workers. This team would visit every household at least once per year, with more frequents assigned based on established patient vulnerability (an insight from the public health side), such as elderly people living alone, or with chronic disease. Medical records and public health targets are also shared and aligned between individual and public health organizations.

By having individual visits, patient information could be assessed for both individual needs and reported to public health authorities at least once per year. Individual and public health directions can then be prioritized accordingly. Further, by having *local* individual visits, the care teams could provide care based on community insight — a patient wouldn't go to get her labwork done on her own, but may well do so if her lab appointment were on the same day as a neighbor's, who would accompany her — an insight that only a local team, fully enmeshed in the community would realize. Universal primary care, "with an emphasis on prevention and public health, [is] now a reality" [2] in Costa Rica, to the substantial benefit of its populace — a mortality rate in Costa Rica of 8.7% compared to 11.2% in the U.S. for people between 15-60 years old, and for the average 60-year old, a life expectancy of an additional 24.2 years in Costa Rica vs. an additional 23.6 years in the U.S. This, for a total health expenditure per person in 2018 of $10,624 in the U.S. vs. $1,337 in Costa Rica.

The key to the success in Costa Rica seems to be the broader public health focus, and *having a contact between public health and individuals, that has (1) deep local knowledge and (2) medical expertise, and is closely aligned with (3) public health goals.* If one were to cast this in cybersecurity terms, it might sound quite appealing. A "public cybersecurity campaign" that cost a lot less than we're spending now and has much broader and greater positive benefit. One could argue that we're already doing this in cybersecurity. For example, we already have a litany of resources from the U.S. Cybersecurity & Infrastructure Security Agency (CISA), identifying "bad practices," listing resources for "cyber hygiene services" such as vulnerability scanning, penetration testing, and running organization phishing campaigns. The challenge is that while these resources may well be having a positive effect, organizations throughout the U.S. have had all of these resources and yet the needle on cybersecurity seems not to have moved.

Mulligan and Schneider have previously examined and extended work in the doctrine of *public cybersecurity* [3], acknowledging computer security as a *public good* given that one compromised system can impact the others around it. So, it makes sense to consider raising the level of security for *everyone* as a public effort.

This brings us to the point of this piece, which is: what would a Salas-style fused public and individual health care system look like for cybersecurity, and how might we achieve such a system? It is not, as I have argued, a simple matter of public information campaigns, which we already have [4]. Nor, I would argue, is it simply surveillance [5] or information sharing, as is commonly enabled through the "Information Sharing and Analysis Centers" (ISACs) created in 1998 through Presidential Decision Directive-63 (PDD-63) to enable public/private information sharing in a variety of critical infrastructure sectors, although both may well help.

So where does this leave us? I've hinted that it is *primary care* — expert connections with individuals, aligned with public health. Who does "primary care" in cybersecurity? Typically, the answer is: a combination of in-house IT security (akin to company doctors and OSHA-required on-site workers) and hired consultants. But there are numerous challenges with the current situation. The first is that qualified in-house security personnel can be very difficult and expensive to hire. Such personnel also are focused on corporate goals rather than an alignment with public health goals, and can certainly have a siloed effect. The focus of corporate IT security can often exacerbate the disparities between the corporate haves (Fortune 500) and the corporate have-nots (everyone else, particularly small businesses and non-profits). Similarly, consultants are also not public-health focused, nor are they local community-focused — consultants are "guns for hire" and are notoriously long-distance road warriors. It is also "virtually impossible for an outsider to tell an expert from a charlatan," [6] though this has improved somewhat with some professional certifications (e.g., CISSP, CISM). The problem is that it is up to individual company to require those. There is no cybersecurity equivalent of the Auditing Standards Board for Certified Public Accountants or the

bar for lawyers.

The solution is perhaps a very different kind of universal primary care for cybersecurity. As Gawande writes, the "priority is "the relationship with the community, not just between the physician and patient."' [2] A few examples of such an approach do exist.

Notable examples are the cybersecurity clinics set up by universities such as UC Berkeley, Indiana University, MIT, and UT-Austin, and non-profits, such as R-Street, which, along with numerous other such clinics, now form a national Consortium of Cybersecurity Clinics [7]. These clinics both seek to provide basic training to a cybersecurity workforce and then to provide hands-on support to "non-profits, hospitals, municipalities, small businesses, and other under-resourced organizations." Google has also provided more than $20 million to support the operation of these clinics, in addition to cybersecurity training and certification via Coursera [8].

Another example, that I happen to be able to claim personal experience with is Trusted CI, the NSF Cybersecurity Center of Excellence [9] *[Full Disclosure: as of October 2024, I am the Director and PI of Trusted CI].* Trusted CI has been funded since 2012 by the U.S. National Science Fondation (NSF) to help secure research cyberinfrastructure to support trustworthy science, which it does through deep engagements, communities of practice, training, publications, webinars, and conferences. Notably, the *Trusted CI Framework* [10] is designed to be an attainable standard for cybersecurity programs, more appropriate for NSF cyberinfrastructure operators than most guidance from the National Institute of Standards and Technology (NIST). Given all of these activities, the composition of its staff, and the presence of that staff in the community, Trusted CI has deep, long-standing relationships with scientific cyberinfrastructure operators throughout the U.S., and particularly many of the NSF Major Facilities — the instruments, such as optical and radio telscopes, supercomputers, maritime research vessels, polar facilities, and Earth science-monitoring networks whose facilities substantially support the research funded by NSF. In many of the ways highlighted by the Costa Rican model, Trusted CI fulfills that vision.

Yet another organization that serves this role is Verified Voting [11], and other groups that support election officials with cybersecurity and related expertise. Members of Verified Voting, for example, have, since 2004, directly supported numerous state and local election officials with direct support for cybersecurity of offices, inspection of voting equipment, and post-election audits.

Organizations supporting whistleblowers and journalists, such as the Electronic Frontier Foundation (EFF), the Committee to Protect Journalists, the Freedom of the Press Foundation, and the Guardian Project, also all provide cybersecurity support, although these organizations provide best practices and resources that can be used by journalists and not necessarily hands-on assistance.

All of these examples have *individual connections* and *local presences* with the organizations that they support, and a *public health focus* as part of their ethos that not only benefits their constituent audiences but can also radiate outwards by virtue of consciousness of the broader public. In this way, we might consider these three organizations to be analogous to a primary care team that "serves as the public health department's 'front door'" [12].

At the same time, at least at this point, the organizations are focused primarily on narrow, albeit importants, sectors. And in the case of cybersecurity clinics, paramedics are not the same as primary care physicians [13]. I argue we need other Cybersecurity Clinics, EFFs, Trusted CIs, and Verified Votings to support vastly more organizations across a comprehensive set of sectors. How might this scale? That is less clear. There are at least two barriers: one is expert cybersecurity personnel, the second is the absence of public-focused institutions in these other sectors. Both face challenges. Despite investments such as the U.S. Government's "CyberCorps: Scholarships for Service" program to recruit and train IT and security professionals, such programs likely need to scale significantly larger. Furthermore, they lack the institutional organization that coordinated public health agencies need. While one could imagine the ISACs, or even CISA, taking on this

role to some extent, in addition to their traditional information sharing, what about the smaller organizations, or even the individuals? That is less obvious.

There is a huge amount of financial support from banks for small business loans, or from state and national agencies for financial contributions to non-profits. Perhaps banks could provide cybersecurity support along with their donations. Perhaps companies providing cyber insurance could provide actual cybersecurity support rather than just a checklist of minimum security requirements and the "promise" [14] of a payout in the event of a successful attack. Perhaps state and national agencies that support non-profits could provide cybersecurity support rather than an unattainable set of NIST guidance.

It should be noted that while these conditions appear necessary, they are not sufficient. Wherever there is a public health system that works, such as Costa Rica's, those systems also comes with mandates and pointed teeth, not just the kindness of the doctor visiting you. In Costa Rica, there are 14 vaccination obligations for children (15, including COVID). The United States is not even close in this regard [15]. The Netherlands, where religious political issues made vaccination recommended rather than required, has 1/3 the number of measles cases of the USA despite of having 1/20th of the population [16], while Costa Rica had zero non-tourist cases for the past decade [17]. In cybersecurity, going back to the point in the opening paragraph of this piece about professional licensing, liability, and disciplinary actions for malpractice, we mostly have neither carrots nor sticks. Perhaps pending legislation in Europe will make similar differences to what GDPR has made, but it will take many years to determine any effect. In addition, perhaps the emphasis on shifting liability to software manufacturers in the Biden Administration's 2021 *Executive Order on Improving the Nation's Cybersecurity* [18] will result in improvement. In the meantime, as an illustration of the effects of the absence of such carrots or sticks: the major European airlines compensated passengers in meals and hotels for the effects of the CrowdStrike update failure. In addition, as of now, CrowdStrike (and Microsoft, to some extent) "apologized" in Congress [19], but has paid nothing in compensation, and has indicated to Delta that it will defend itself against any legal claims [20].

But the threat of cyberattacks against organizations that power society is too significant to throw our hands up. A risk-management approach with layers of strategies could help. Indeed, many of the same approaches that private health systems might employ to benefit public health [12] could also be adapted to benefit a public and community centric cybersecurity ethos, including:

- Targeting public funding to support non-profits addressing the most readily preventable cyberattacks.
- Having local or regional "cybersecurity clinics" and leverage cyber "telehealth" to areas without a critical mass of population to support such clinics.
- Leveraging the first to points, build capabilities to "assign" non-profits and key small businesses a "cyber primary care" representative. This is not unlike the approach taken by the local Auxiliary Communications Service that I am involved with in supporting local Community Based Organizations (e.g., food banks, homeless shelters) that have important public functions, particularly in emergencies.
- Computer science departments can expand curricula to include a "public health" ethos in the same way that ethics curricula have expanded over recent years.
- Strong means of determining experts from charlatans.

- Identifying, enacting, and enforcing "carrots" and "sticks" to ensure the widespread and effective implementation of public health equivalents.

All models are wrong, but some are useful. The adversaries in medicine are bacteria and viruses while the adversaries in cybersecurity are humans. To what degree will the comparative intelligence of those adversaries negatively affect the effectiveness of a public health model? Past models have shown some successes in leveraging a public health analogy to cybersecurity but serious gaps remain, and there is more that must be explored. Perhaps Salas's Costa Rican public health model, adapted to cybersecurity, is now worth trying, too.

Acknowledgements: My sincere thanks to Fabio Massacci and Jianying Zhou for their invaluable feedback on and contributions to this piece, which has materially improved this end product.

References

[1] Charles-Edward Amory Winslow. The Untilled Fields of Public Health. *Science*, 51(1306): 23–33, 1920. doi:10.1126/science.51.1306.23.

[2] Atul Gawande. Annals of Medicine: Costa Ricans Live Longer Than Us. What's the Secret? *The New Yorker*, August 23, 2021.

[3] Deirdre K. Mulligan and Fred B. Schneider. Doctrine for Cybersecurity. *Daedalus*, 140(4): 70–92, 2011. doi:10.1162/DAED_a_00116.

[4] Cybersecurity & Infrastructure Security Agency. Shields Up! `https://www.cisa.gov/shields-up`.

[5] Jeff Rowe, Karl Levitt, and Mike Hogarth. Towards the Realization of a Public Health System for Shared Secure Cyber-Space. In *Proceedings of the 2013 New Security Paradigms Workshop*, pages 11–18, Banff, Canada, September 9–12, 2013. doi:10.1145/2535813.2535815.

[6] Ross Anderson. Why Cryptosystems Fail. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pages 215–227, 1993. doi:10.1145/168588.168615.

[7] The Consortium of Cybersecurity Clinics. `https://cybersecurityclinics.org`.

[8] Google.org. Google Cybersecurity Clinics Fund: Investing in America's cybersecurity workforce. `https://cyberclinics.withgoogle.com`.

[9] Andrew Adams, Kay Avila, Jim Basney, Dana Brunson, Robert Cowles, Jeannette Dopheide, Terry Fleury, Elisa Heymann, Florence Hudson, Craig Jackson, Ryan Kiser, Mark Krenz, Jim Marsteller, Barton P. Miller, Sean Peisert, Scott Russell, Susan Sons, Von Welch, and John Zage. Trusted CI Experiences in Cybersecurity and Service to Open Science. In *Proceedings of the Practice and Experience in Advanced Research Computing (PEARC)*, Chicago, IL, July 28–August 1, 2019. ACM. doi:10.1145/3332186.3340601.

[10] Craig Jackson, Bob Cowles, Scott Russell, Emily K. Adams, Ryan Kiser, Ranson Ricks, and Anurag Shankar. The Trusted CI Framework Implementation Guide for Research Cyberinfrastructure Operators. `https://zenodo.org/doi/10.5281/zenodo.4562446`, March 1, 2021.

[11] Verified Voting. `https://verifiedvoting.org`.

[12] Kathryn C. Peisert. Learning from Costa Rica: Creating Public Health from the Ground Up. *System Focus*, November 2021. The Governance Institute.

[13] Eric Geller. The Bold Plan to Create Cyber 311 Hotlines. *Wired*, June 7, 2023.

[14] Jessica Lyons Hardcastle. Insurers can't use 'act of war' excuse to avoid Merck's $1.4B Not-Petya payout. *The Register*, May 3, 2023.

[15] Our World in Data. Which countries have mandatory childhood vaccination policies? `https://ourworldindata.org/grapher/mandatory-childhood-vaccination`, 2021.

[16] Bartosz Lisowski, Steven Yuvan, and Martin Bier. Outbreaks of the measles in the dutch bible belt and in other places–new prospects for a 1000 year old virus. *Biosystems*, 177:16–23, 2019. doi:10.1016/j.biosystems.2019.01.003.

[17] World Health Organization. Global Health Observatory: Measles - number of reported cases. `https://www.who.int/data/gho/data/indicators/indicator-details/GHO/measles---number-of-reported-cases`, 2024.

[18] Joseph R. Biden Jr. Executive Order (EO) 14028 — Improving the Nation's Cybersecurity. `https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/`, May 12, 2021.

[19] Blake Montgomery and Johana Bhuiyan. CrowdStrike apologizes for global IT outage in Congressional testimony. *The Guardian*, September 24, 2024.

[20] Nadine Yousif. Delta Airlines hits out at CrowdStrike, alleging $500m loss. *BBC News*, August 8, 2024.