PUBLIC HEALTH & CYBER PUBLIC HEALTH

Technical Report 22-01

Translating the lessons of public health to cybersecurity

Prepared by the CyberGreen Institute
March 2022

TABLE OF CONTENTS

1. Executive Summary....4
Key Lessons....4
Takeaways....4
2. Learning from Introduction to Public Health....5
Part I: What Is Public Health?....5
Public Health: Science, Politics, Prevention (Chapter 1)....5
Cybersecurity Perspective....6
Why is Public Health Controversial? (Chapter 2)....7
Cybersecurity Perspective....7
Powers and Responsibilities of Governments (Chapter 3)....8
Structures and Responsibilities....8
Political Factors....8
Statistics....8
Cybersecurity Perspective....9
Part II: Analytical Methods of Public Health....9
Epidemiology: The Basic Science of Public Health (Chapter 4)....9
How Epidemiology Works....9
How Epidemiology Works: Cybersecurity Perspective....10
Epidemiology and the Causes of Chronic Disease....10
Chronic disease and cybersecurity....10
Epidemiologic Principles and Methods (Chapter 5)....11
Kinds of Epidemiologic Studies....11
Cybersecurity Perspective....11
Problems and Limits of Epidemiology (Chapter 6)....12
Cybersecurity Perspective....13
Statistics: Making Sense of Uncertainty (Chapter 7)....13
Cybersecurity Perspective....13
The Role of Data in Public Health (Chapter 8)....14
Cybersecurity Perspective....14
Part III: Biomedical Basis of Public Health....15
The "Conquest" of Infectious Diseases (Chapter 9)....15
Cybersecurity Perspective....16
Resurgence of Infectious Disease (Chapter 10)....17

Cybersecurity Perspective 17
The Biomedical Basis of Chronic Diseases (Chapter 11) 17
Cybersecurity Perspective 18
Genetic Diseases and other Inborn Errors (Chapter 12) 19
Cybersecurity Perspective 19
Part IV: Social and Behavioral Factors in Health 19
Do People Choose Their Own Health? (Chapter 13) 19
Cybersecurity Perspective 20
How Psychosocial Factors Affect Health Behavior (Chapter 14) 20
Cybersecurity Perspective 21
Public Health Enemy Number One: Tobacco (Chapter 15) 21
Cybersecurity Perspective 22
Public Health Enemy Number Two (and Growing): Poor diet and physical inactivity (Chapter 16) 23
Cybersecurity Perspective 23
Injuries are Not Accidents (Chapter 17) 23
Author's Perspective 24
Cybersecurity Perspective 24
Maternal & Childhood Health as a Social Problem (Chapter 18) 25
Cybersecurity Perspective 25
Mental Health (Chapter 19) 26
Part V: Environmental Issues in Public Health 26
A Clean Environment: The Basis of Public Health (Chapter 20) 26
Cybersecurity Perspective 27
Clean Air: Is it safe to breathe? (Chapter 21) 27
Cybersecurity Perspective 27
Clean Water: A Limited Resource (Chapter 22) 28
Cybersecurity Perspective 28
Solid and Hazardous Waste: What to do with the garbage? (Chapter 23) 28
Safe Food and Drugs: An Ongoing Regulatory Battle (Chapter 24) 28
Cybersecurity Perspective 29
Population: The Ultimate Environmental Health Issue (Chapter 25) 30
Part VI: Medical Care and Public Health 30
Is the Medical Care System a Public Health Issue (Chapter 26) 30
Cybersecurity Perspective 30

Why the US Medical System Needs Reform (Chapter 27) 31
Health Services Research: Finding What Works (Chapter 28) 31
Cybersecurity Perspective 32
Public Health and the Aging Population (Chapter 29) 33
Cybersecurity Perspective on Part VI 33
Part VII: The Future of Public Health 33
Emergency Preparedness, Post 9/11 (Chapter 30) 33
Cybersecurity Perspective 33
Public Health in the 21st Century: Achievements and Challenges (Chapter 31) 34
Cybersecurity Perspective 34
3. Conclusion 35
References 36
Acknowledgements 38

1. EXECUTIVE SUMMARY

This project was undertaken to provide a structured approach to the question "How can we systematically translate the lessons of public health to cybersecurity?" This paper uses a popular textbook, Mary-Jane Schneider's *Introduction to Public Health (6th ed)* as a structure to answer the question, following Dr. Schneider's understanding of that field. Comparisons between cybersecurity and health are legion — we speak of computer viruses, despite their lack of RNA. And of course, analogies all have limits.

KEY LESSONS

There are a number of key lessons from the project. The first is that public health exists in tension with other values. While none of us want contaminated drinking water, sometimes providing safe water is expensive. None of us want contaminated food, but the steps to prevent contamination can be expensive, and making food more expensive has other health impacts. Some possible steps, like irradiation, can lead to people being concerned and avoiding safer, healthier irradiated vegetables.

The second is that public health, like cybersecurity, is a broad field that can touch on, or be a lens through which to view many different parts of life. That means that it can be hard to "nail down" what public health "really is."

TAKEAWAYS

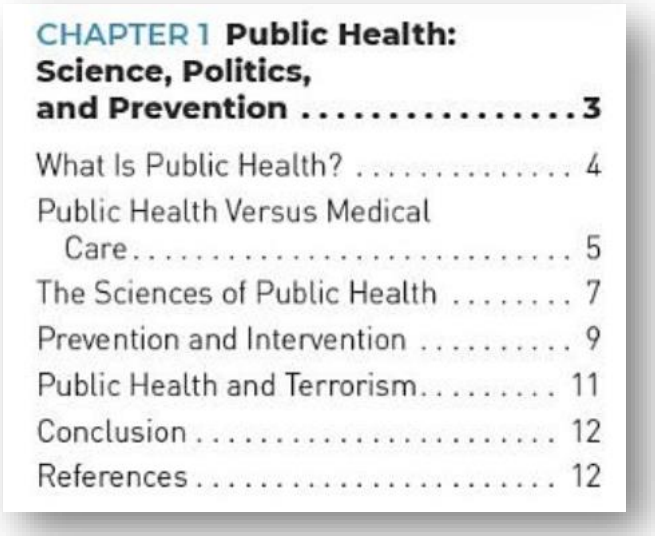
- Public health framing has had a dramatically positive effect on the human experience. The average American lives decades longer than they did at the start of the 20th century.
- Need for proof points. Public health has many proof points, from the Broad Street pump through the years of life expectancy gained in the 20th century. If we are going to develop a parallel discipline, we will need proof points.
- Value and breadth of data. There are a great many data sources used by public health, gathered with more rigor, more mandates, and more uses than we have in cybersecurity.
- Limits of what is possible. There are areas, including weight loss, tobacco, and automotive safety, where massive improvements in years of healthy life are clearly achievable, at a cost that individuals or society is not willing to pay.
- Complexities of regulation are a result of there being a myriad of financial interests in selling products that either heal or harm people, or in keeping costs down. There are also important issues of framing and "what is the proper role of government", along with the perception that something is either an individual choice, or that those choices are shaped by societal messages and hard to resist.

Despite the limits of analogies, this project shows that a great many elements of cyber public health should be pursued.

2. LEARNING FROM INTRODUCTION TO PUBLIC HEALTH

PART I: WHAT IS PUBLIC HEALTH?
PUBLIC HEALTH: SCIENCE, POLITICS, PREVENTION (CHAPTER 1)

We start from the basic question: "what is public health" and an acknowledgement that public health is hard to define and frequently misunderstood. "Leaders in the field have themselves struggled to understand the mission of public health..." This makes for a worrisome start! If they do not know what they are, why should we be emulating them? The simple answer is "the general state of people's health is now much better than it was [200 years ago]" and "the measures that people take as a society" contribute to that success.


CHAPTER 1 **Public Health: Science, Politics, and Prevention 3**
What Is Public Health? 4
Public Health Versus Medical Care 5
The Sciences of Public Health 7
Prevention and Intervention 9
Public Health and Terrorism 11
Conclusion 12
References 12

A National Academies report, *The Future of Public Health*, defined ten essential functions in three main areas: Assessment, policy development and assurance:

Assessment

1. Monitor health status to identify community health problems
2. Diagnose and investigate health problems and health hazards in the community

Policy Development

3. Inform, educate and empower people about health issues
4. Mobilize community partnerships to identify and solve health problems
5. Develop policies and plans that support individual and community health efforts

Assurance

6. Enforce laws and regulations that protect health and ensure safety
7. Link people to needed personal health services and assure the provision of health care when otherwise unavailable
8. Assure a competent public health and personal healthcare workforce
9. Evaluate effectiveness, accessibility and quality of personal and population-based health services.

Serving all functions

10. Research for new insights and innovative solutions to health problems.

Public health acts as a frame for a coalition with many professional disciplines, covered in depth later in the book and in this paper. Public health is generally concerned with interventions, designed to address problems:

1. Define a specific health problem
2. Identify the risk factors associated with the problem
3. Develop and test community-level interventions to control or prevent the cause of the problem.
4. Implement interventions to improve the health of the population
5. Monitor those interventions to assess their effectiveness

There are primary interventions, involving preventing exposure to risk factors, secondary interventions to minimize the severity of the problem, and tertiary interventions which seek to minimize disability.

CYBERSECURITY PERSPECTIVE

Each chapter review will have at least one cybersecurity perspective section. For a few chapters, it will make sense to break it up. This one, unusually, will start with a note about public health and its relationship to medicine: "Whereas medicine is concerned with individual patients, public health ... tries to improve the health of the population. Medicine focuses on patients who are ill, public health focuses on preventing illness." This serves to help us see some important distinctions:

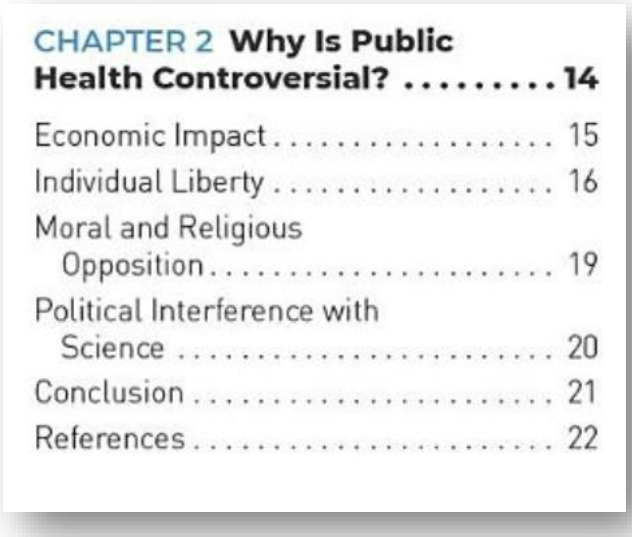
Some major differences between public health and cybersecurity are that:

- Cybersecurity typically crosses that boundary of "illness/preventing illness," focusing on protection, detection and response. For example, a firewall is focused on preventing problems, and anti-virus software traditionally tries to prevent a virus from getting into a system
- Cybersecurity incidents are most frequently caused by some intelligent agent and their intentional activity.
- Businesses play very different and perhaps more meaningful role in cybersecurity defenses than in public health. Most obviously, people get sick, businesses do not, but both people and businesses can own computers that experience security issues.
    - The issues that a firm faces with its computers can directly impact the firm's bank accounts or ability to make and sell products or deliver services. While food suppliers and restaurants are directly and specifically regulated because of the many food-borne illnesses, every business has to act to integrate cybersecurity into its operations.
    - Businesses create most software, while people create people. The investments that each make are different: businesses seek to minimize costs and maximize profits, while people seek to give their children good lives. A very small set of businesses make software that is very widely used, and their investments impact the defenses of a great many organizations.
- Security problems often span across people and organizations in ways health issues do not. For example, when my credit card is stolen from firm A, that can impact me, my bank, and firm B where my card is fraudulently used. Similarly, but not identically, if my password is stolen, that may impact my account at site B. And if my SSN is stolen, that can have long term repercussions for me across many organizations.

WHY IS PUBLIC HEALTH CONTROVERSIAL? (CHAPTER 2)

As a goal, public health is hard to argue with. Who would not want clean water, or freedom from pollutants? But not all interventions are so broadly desirable: many people are opposed to sex education in schools for religious reasons. Others are opposed for cost reasons. Reducing pollution has a cost for the polluter, while bar owners broadly expected that banning smoking would reduce drinking.

Regulation also has a cost. Keeping a restaurant kitchen clean has a cost, and some cookbook authors have argued that, for example, government rules on safe temperatures for pork long required overcooking it to handle a very rare disease, or that rules for cheeses are far stricter than those in Europe (Hay 2018; Myhrvold 2011).


CHAPTER 2 **Why Is Public Health Controversial? 14**
Economic Impact 15
Individual Liberty 16
Moral and Religious Opposition 19
Political Interference with Science 20
Conclusion 21
References 22

CYBERSECURITY PERSPECTIVE

Cybersecurity similarly has elements which make improvements controversial. Security appears to take energy away from things which directly make money. Security has a cost: changing passwords, applying patches and rebooting, and dealing with access controls that keep people out.

POWERS AND RESPONSIBILITIES OF GOVERNMENTS (CHAPTER 3)

STRUCTURES AND RESPONSIBILITIES

The chapter on governments starts with a brief discussion of the split between federal and state authority and comments that "all states have laws such as mandates to collect data about the population, to immunize children before they enter school, to regulate the environment for purposes of sanitation, and to regulate safety." It goes on to discuss the power struggles between the states and the Federal government. One example is tying highway funding to motorcycle helmet laws in the 1970s, and how in the 1980s there was a movement to "return power to the states" which led to a reversal of such laws, and allowed road deaths to rise.


CHAPTER 3 Powers and Responsibilities of Government 23
Federal Versus State Authority 24
How the Law Works 25
How Public Health Is Organized and Paid for in the United States . . . 27
Local Public Health Agencies 27
State Health Departments 27
Federal Agencies Involved with Public Health 29
Nongovernmental Role in Public Health 33
Conclusion 34
References 35

Most of the Federal government's health powers are concentrated in the department of Health and Human Services, including the FDA, CDC and National Institutes of Health. Other agencies including at least the EPA and DoE have substantial influence on the environment and thus health, and the Department of Veteran's Affairs is responsible for health care for millions.

POLITICAL FACTORS

Tobacco and firearms clearly implicate public health issues, and they have supporters in Congress. This limits the ability of public health officials to regulate them, or, in the case of firearms, to even study the causes of gun violence (Rostron 2018). Congress has similarly, but less intensively, questioned if cybersecurity regulation represents needless red tape.

STATISTICS

The world of public health is, comparatively, awash in statistics, including the CDC's Morbidity and Mortality Weekly Report, OECD statistics such as https://www.oecd.org/health/health-at-a-glance/, or your favorite COVID data tracker. Try finding a reliable and consistently updated report on how many phishing emails were sent last week.[1] A useful survey of public heath reporting is in (Sedenberg 2015).

[1] There is a monthly report at the Center for Internet Security, and I've just emailed them to ask why their graphs have no labels. https://www.cisecurity.org/blog/top-10-malware-december-2021/

CYBERSECURITY PERSPECTIVE

Cybersecurity also has evolved a system of responsibilities, including regulation and enforcement at the state and even local levels, although it is more haphazard. Many of these regulations have been promulgated because of disagreements about, for example, the nature of breach reporting.

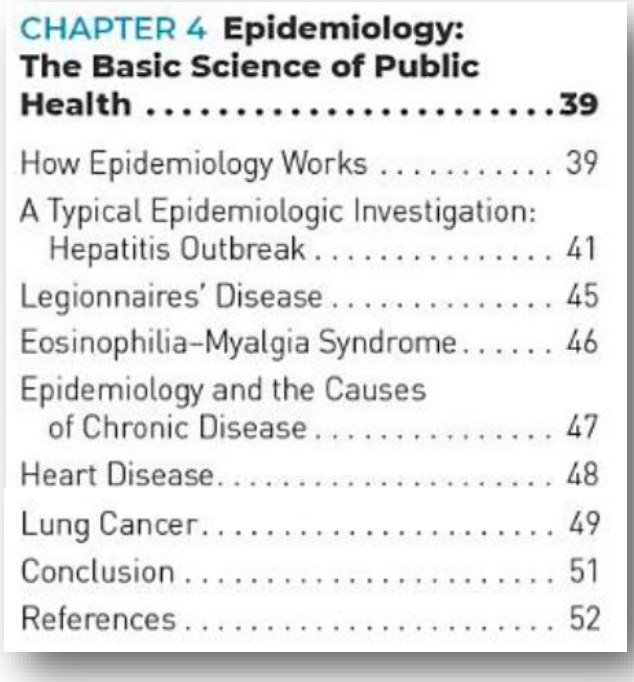
The Federal government has numerous agencies with some broad cybersecurity responsibility, including NIST, DHS/CISA, FTC, FBI, Secret Service, and many sectoral agencies, including the FDA, Department of Defense, and HHS issuing sectoral cybersecurity regulation at a dizzying pace.

PART II: ANALYTICAL METHODS OF PUBLIC HEALTH EPIDEMIOLOGY: THE BASIC SCIENCE OF PUBLIC HEALTH (CHAPTER 4)

Epidemiology is the diagnostic discipline of public health, and was originally focused on epidemics: an increase in the frequency of disease above some endemic (usual) rate. The text discusses the example of how, in 1853, John Snow was able to distinguish the correlation of cholera deaths per household with water supplied by various companies. To do so, he took advantage of the British government's new routine collection of birth and deaths, which had started 14 years earlier.

HOW EPIDEMIOLOGY WORKS

Governments operate epidemiologic surveillance to understand a possible outbreak early. There are a set of notifiable diseases – roughly 90 defined by the federal government and more in some states. All physicians, hospitals and labs are required to notify their local health authorities, and those health authorities notify the CDC. Notably, the author asserts that "the first step in recognizing that a community is facing a new problem is usually a report to the local or state health department or the CDC by a perceptive physician who notices something unusual that he or she thinks should be investigated further."


CHAPTER 4 **Epidemiology: The Basic Science of Public Health** **39**
How Epidemiology Works 39
A Typical Epidemiologic Investigation: Hepatitis Outbreak 41
Legionnaires' Disease 45
Eosinophilia-Myalgia Syndrome 46
Epidemiology and the Causes of Chronic Disease 47
Heart Disease 48
Lung Cancer 49
Conclusion 51
References 52

There is an extended discussion of three typical investigations, using hepatitis, legionnaire's disease and Eosinophilia-Myalgia caused by food supplements. Investigators start with the who, where, and when questions of the identified victims. The how is an understood aspect of the disease. For example, in the case of hepatitis, it is transmitted in food and water.

HOW EPIDEMIOLOGY WORKS: CYBERSECURITY PERSPECTIVE

Cybersecurity does not have routine statistical data collection, and it is unclear what the equivalents of births and deaths might be. (New purchases of computers would be one analog for birth, and new computers are often configured to be much like the one they are replacing, so that makes the analogy less close.)

Diseases are also unclearly defined – "malware families" are generally defined by commercial firms who rarely publish their criteria for naming something a new strain.

In cybersecurity, there is no body charged with accepting professional reports of unusual conditions and investigating further.[2] What would be counted as unusual, or how many requests for expertise might come in are open questions. As I write this, I have a concern that a great many requests for expertise might flood in, and I believe that is indicative of a possible failure in the market for investigative tooling.

EPIDEMIOLOGY AND THE CAUSES OF CHRONIC DISEASE

The section opens on the difference between chronic disease, such as cancer or heart disease, and diseases caused by infectious agents. These diseases are more difficult to study than acute outbreaks, and so the methods used are different. Many of these diseases were once thought to be symptoms of aging.

There are risk factors that contribute to the development of diseases, and these are studied in prospective cohort studies, such as the Framingham Study and the British Smoking Survey. These large studies are expensive and take time. The Framingham Study began with 5,000 people in 1948, and derivative studies are ongoing. As of 2004, only 534 participants remained alive, the youngest of whom was 84. These large studies have had dramatic impacts on public health, driving down rates of heart disease and smoking.

The British Smoking Studies, started in 1950 and 1952, had a dramatic impact on the rates of smoking (falling to less than half the number of cigarettes smokes per day), and the study ended in 1971.

CHRONIC DISEASE AND CYBERSECURITY

It is well known that computers show symptoms of age. These differ from issues when they've been on too long, and errors have accumulated that can be fixed by rebooting them. These symptoms include physical and software failures (those that are fixed by re-installing). Physical failures include connectors or power supplies going bad, etc. The question of software aging is provocative: why does software age, what is the relationship of age with configuration, and what might we expect in terms of software lifespans? There's a current movement to "treat systems like crops, not pets." This means that in a data center, we plant and reap the operating system and other software on that computer hardware or virtual machines regularly, rather than trying to maintain them.

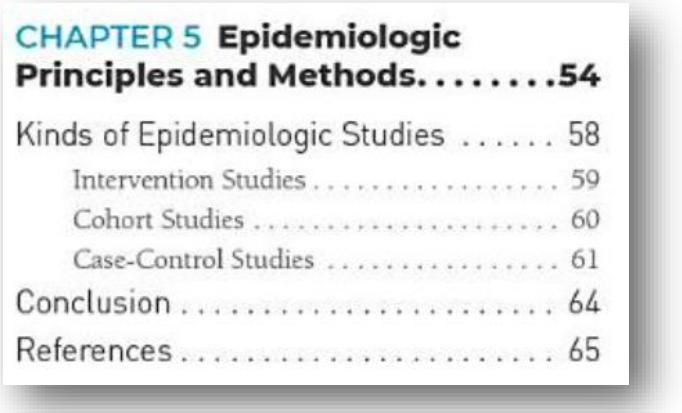
[2] CERTs are charged with assisting and information sharing, and may, for example, do some malware analysis, but do not do additional investigation of the original problem within the original targeted network.

EPIDEMIOLOGIC PRINCIPLES AND METHODS (CHAPTER 5)

"Epidemiology is defined as 'the study of the distribution and determinants of disease frequency in human populations.' Each of those terms must be clearly understood."

Clear definitions are important. Sometimes, this is easy (gunshot wounds) and other times harder (hepatitis is one of many diseases which presents with vomiting and diarrhea, so a blood test is called for.) The definition of population at risk is important – for example, ovarian cancer is calculated relative to the female population, not a total population. The incidence is the new cases in a defined population per time, while probability is the chance a healthy person will develop the disease, and prevalence is the number of cases in a population. At the risk of repetition, we lack the data for addressing these in cybersecurity.

KINDS OF EPIDEMIOLOGIC STUDIES


CHAPTER 5 Epidemiologic Principles and Methods. 54
Kinds of Epidemiologic Studies 58
Intervention Studies 59
Cohort Studies 60
Case-Control Studies 61
Conclusion 64
References 65

We can divide studies into intervention studies, cohort studies, and case-control studies. They can be prospective (following a group to see who develops a disease) or retrospective (starting from a group suffering from a disease and looking back). An intervention study is where an intervention is tested for effectiveness, and this is where terms like randomization (ensuring that people are in a treatment or control group is random), and double blind come into play. Double-blind means neither the patient nor the physician knows which group a person is in. A cohort study is like the Framingham Study where a set of people are followed for an extended period of time.

CYBERSECURITY PERSPECTIVE

Intervention studies are a place where cybersecurity finally has an advantage. We can assess the quality of a fix in a lab setting with relatively high reliability. The computer rarely cares you're observing it. We need way fewer computers to be in a test, and, assuming code is flawless, they comply with the experimental protocol. However, intervention studies may still be useful to assess compliance with advice – how many people apply a patch, how quickly and how reliably?

In contrast, cohort studies are rare. Enrolling systems and checking on them creates complex challenges. Also, the shared understanding of types of experiments and measures of effectiveness that public health has are sorely lacking in cybersecurity. For systems which operate in the cloud, what would make up a cohort is more complex than a world in which "gold master" systems are repeatedly installed and then used for years.

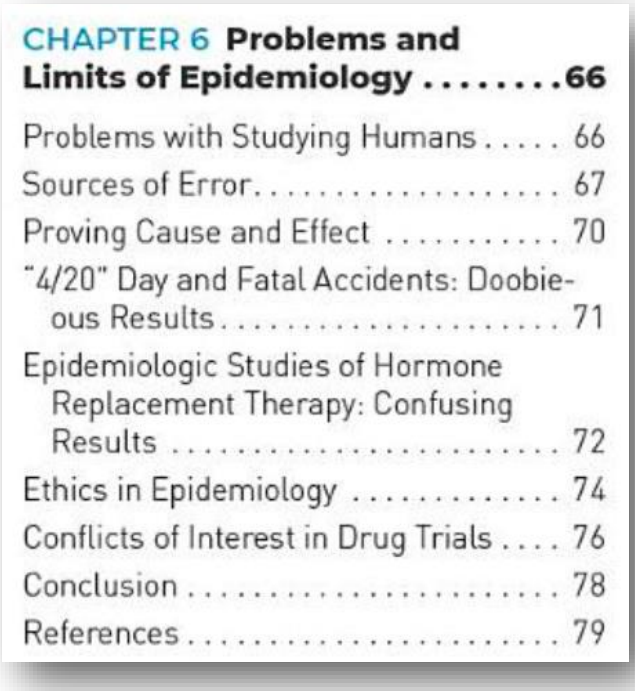
For example, in cybersecurity it is somewhat normal to make statements like "Zero trust is expected to double the average efficacy of cybersecurity protections against a range of threats and incident

types" (Osterman Research 2021). The measurement was the number of survey respondents who expected their confidence in their security measures to prevent various attacks to move to "confident or highly confident." The precise question was not disclosed, nor was the range of possible answers. The prior question had "highly impactful" and "extremely impactful" as the answers revealed. Was there an "extremely confident" in this question? This white paper was one that I came across randomly, and I do not mean to pick on it. Such quality issues are endemic in cybersecurity surveys.

PROBLEMS AND LIMITS OF EPIDEMIOLOGY (CHAPTER 6)

The chapter opens with the problems of studying humans, and uses the example of a change in diet. It is hard to get people to sign up for an intervention study to change their diet for an extended period. (Compare and contrast with rats in cages whose diets can be precisely controlled.) It is hard to know in a cohort study if the people who are eating a lower fat diet have other factors in common.

There are understood groups of causes of error. These include random variation, confounding variables, and biases. There are known ways of overcoming these errors, and those methods are not free. For example, the British smoking studies involved tens of thousands of doctors and showed large effects. The larger study means that random variation should not cause the study to show different results than the whole population. Controlling for confounds and other biases involves careful study design and analysis, as well as careful selection and matching of participants. Such care takes time and thus money. Another form of bias is in survey responses: some surveys get low response rates, and it may be that the people who fill them out are biased. I am certainly more likely to fill out a customer satisfaction survey when angry.


CHAPTER 6 **Problems and Limits of Epidemiology 66**
Problems with Studying Humans 66
Sources of Error. 67
Proving Cause and Effect 70
"4/20" Day and Fatal Accidents: Doobie-ous Results 71
Epidemiologic Studies of Hormone Replacement Therapy: Confusing Results 72
Ethics in Epidemiology 74
Conflicts of Interest in Drug Trials 76
Conclusion 78
References 79

The chapter continues with a discussion of why proving cause and effect is hard and some of the ways that epidemiologists overcome them. Those include large studies, a strong association between exposure and disease, a dose-response relationship, and a known explanation for the effect being studied. (It turns out that why cigarettes cause cancer is still poorly understood, but the other factors create convincing evidence.)

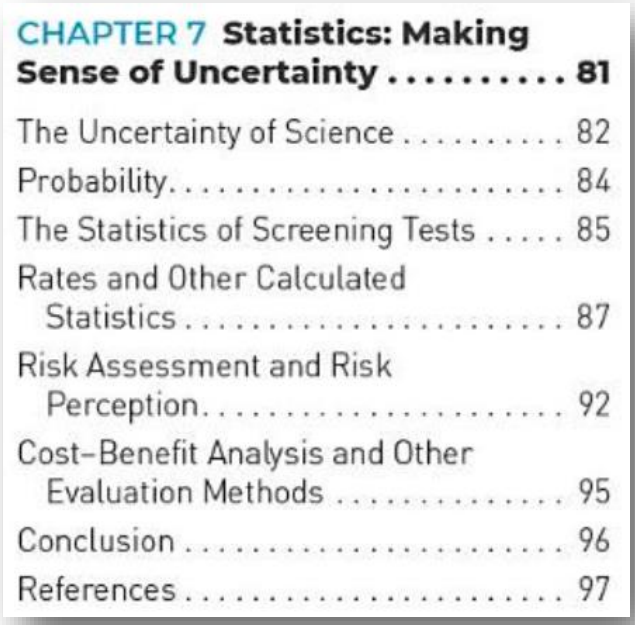
The chapter continues into an extended discussion of an alleged relationship between "4/20 day" and fatal accidents, and then into the confusing results of studies of hormone replacement therapy. From there, it touches on ethics and conflict of interest.

CYBERSECURITY PERSPECTIVE

Many of the issues translate nicely. The ability to carefully review results is sometimes present in studies which are published academically. Cybersecurity is different from epidemiology insofar as there is a great deal of enthusiast research, and such research is often credible. Cybersecurity problems like "can I find a vulnerability in this software" are the sorts of things one can explore in a home lab. It may be that enthusiast research is less feasible in cyber public health than in cybersecurity.

STATISTICS: MAKING SENSE OF UNCERTAINTY (CHAPTER 7)

The opening of the chapter struck me: "In fact, all public health, because it is concerned with populations, relies on statistics to provide and interpret data." There is an extended section on the uncertainty of science, and that even with data from population statistics and carefully managed studies, those studies are sometimes contradictory. Worse, sometimes the statistics come at odds with the desire of populations. She relates the story of controversy after controversy over when to start screening for breast cancer.


CHAPTER 7 Statistics: Making Sense of Uncertainty 81
The Uncertainty of Science 82
Probability. 84
The Statistics of Screening Tests 85
Rates and Other Calculated Statistics 87
Risk Assessment and Risk Perception. 92
Cost–Benefit Analysis and Other Evaluation Methods 95
Conclusion 96
References 97

The chapter continues with a discussion of probability, the use of statistics in screening tests (along with challenges), rates and other calculations, with a section on how different measures tell very different stories. That section shows that the crude death rate per 100,000 is substantially higher (970 in Florida vs. 596 in Alaska in 2017), while the age-adjusted rates "tell a different story" with 672 in Florida vs. 708 in Alaska. She also discusses measures like Years of Potential Life Lost (YPPL) which is a measure designed to illustrate those causes that kill younger people. She continues into risk assessment vs risk perception, and cost benefit analysis and other evaluation methods.

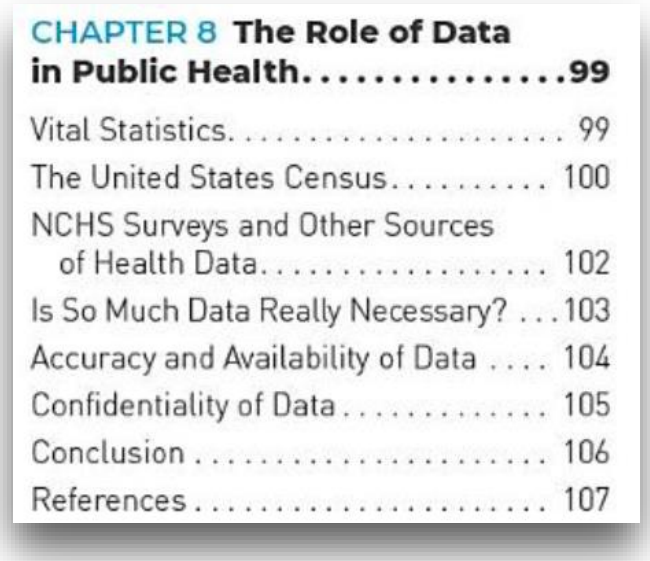
CYBERSECURITY PERSPECTIVE

As I was drafting this paper, the FBI issued a "FLASH Alert" about flash drives being mailed to businesses (Gatlan 2022; Lyngaas 2022). To the best of my ability to understand, there is no mention of base rate, no mention of change in rates, no description of the population at risk. So, it is not clear why the alert was worth issuing. In contrast, there are reasonably clear guidelines as to what constitutes an epidemic, an outbreak or a pandemic.

THE ROLE OF DATA IN PUBLIC HEALTH (CHAPTER 8)

There is a National Center for Health Statistics within the CDC, and it has two main modes of data collection: reports from states and surveys. Surveys include the US Census and a variety of telephone and in person surveys.

Vital statistics include births and deaths. Much of the information associated with a birth certificate is so confidential it is not even available to the subject of the certificate, including labor and delivery complications or abnormalities. It is collected and used solely for public health reasons. Information on death certificates has a number of sources of inaccuracy, including elderly people who leave no survivors to providing information on parents, education or occupation. They also include misdiagnoses and misreporting of diagnoses (AIDS, suicide) to avoid stigma.


CHAPTER 8 The Role of Data in Public Health.....99
Vital Statistics..... 99
The United States Census..... 100
NCHS Surveys and Other Sources of Health Data..... 102
Is So Much Data Really Necessary? ...103
Accuracy and Availability of Data 104
Confidentiality of Data..... 105
Conclusion..... 106
References..... 107

There is a section titled "Is so much data really necessary?" and the answer is a resounding yes, for both research and surveillance (in the sense of detecting new outbreaks). Another section, titled "accuracy and availability" covers the challenges of data quality and a final section covers confidentiality.

CYBERSECURITY PERSPECTIVE

The most basic of "vital statistics" include births and deaths – we do not have either. Phones are somewhat easier because they're generally not modified or changed substantially. It is somewhat easy to say that a phone is "born" either when it is manufactured or when it is activated. What about when it is wiped and sold to someone else? Is that a death and a birth? With a "classic tower PC", is swapping a hard drive a new birth? Re-installing from install media? What about a cloud computing instance which is managed with a "machine image"? Is the creation of the machine image a birth? Its being stood up and run? What is the relationship between death and a system being decommissioned, or the hardware/software it uses being marked "end of life?"

A few examples: It is hard to get a count of IOT devices out there, or sold in a given year. For example, for 2020, IOT Analytics lists 11.7B, while Statista lists 8.74B, and Security Today quotes a claim of 31 billion expected. The correct answer is less important than the fact that 1 billion infected devices is either 12% or 3% of all devices, depending on if we believe Statista or Security Today. Our understanding of the prevalence of the problem, or the probability that a new device will be impacted are reliant on these numbers.

Another example: when I worked at Microsoft, I was unable to find data on how many Windows computers there were. I did see data on Windows Update, which is a subset of consumer computers

running Windows, many of whose users turn off automatic update. Enterprises usually manage updates, and so they are excluded from such data. I might have been able to find data on license sales, complicated by say, Dell, selling a computer to a company with an enterprise license.

The question of "is so much data really necessary" is a fascinating one, and raises the question, how can we prove a need for more data? Perhaps part of the answer lies in our inability to assess how we're doing, or in the inability to overcome inhibitions.

PART III: BIOMEDICAL BASIS OF PUBLIC HEALTH
THE "CONQUEST" OF INFECTIOUS DISEASES (CHAPTER 9)

The chapter opens with a graph of death rates in NYC 1800-2017, showing that deaths per 1,000 have fallen from an average of 20-30 through the 1800s to roughly 10 in the 1900s. The end of the 1800s were an explosion of scientific knowledge of pathogens, and how to address them. They were addressed through a combination of techniques including water purification, sewage management, milk pasteurization and immunization. The effectiveness of these techniques seemed to reduce infection to a nuisance by the 1960s.

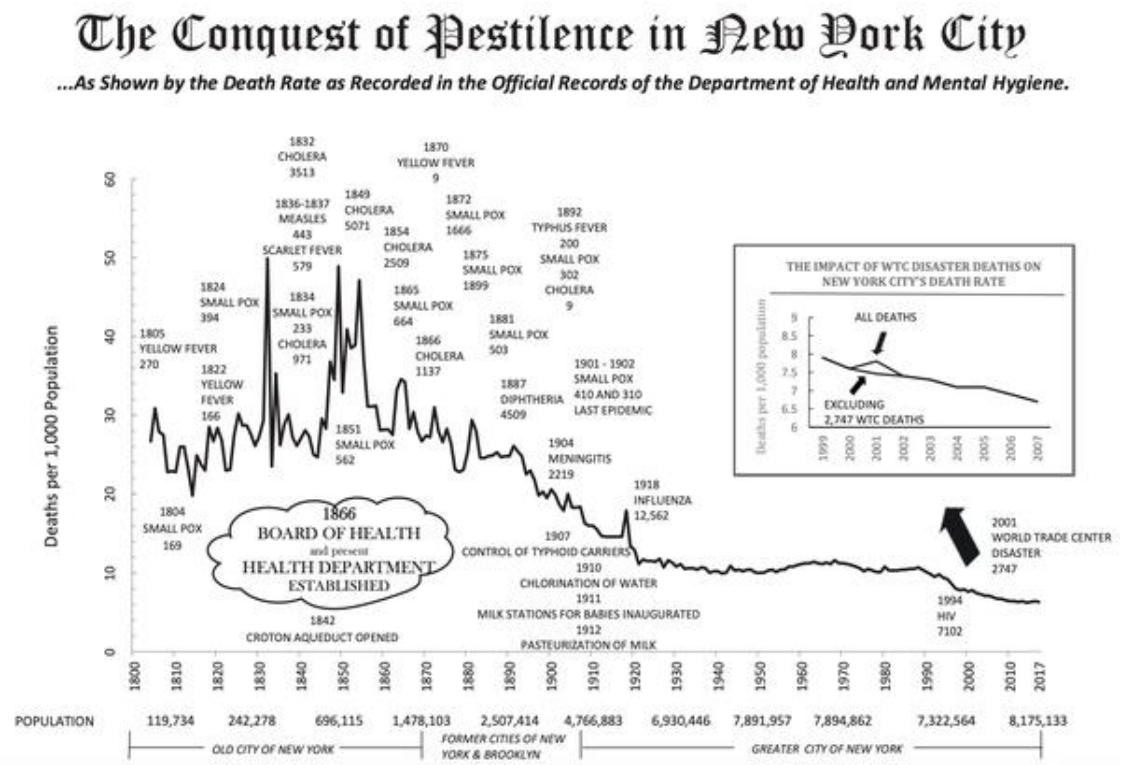


Figure 1: Deaths in NYC

One of the keys was scientific and then public agreement on both means of transmission (by bacteria, viruses or parasites), the precise definition of an infectious agent, and a model of the chain of infection. (The model, shown in is reasonably self-explanatory.)

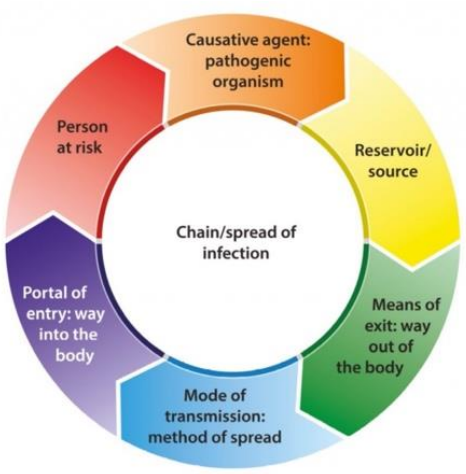


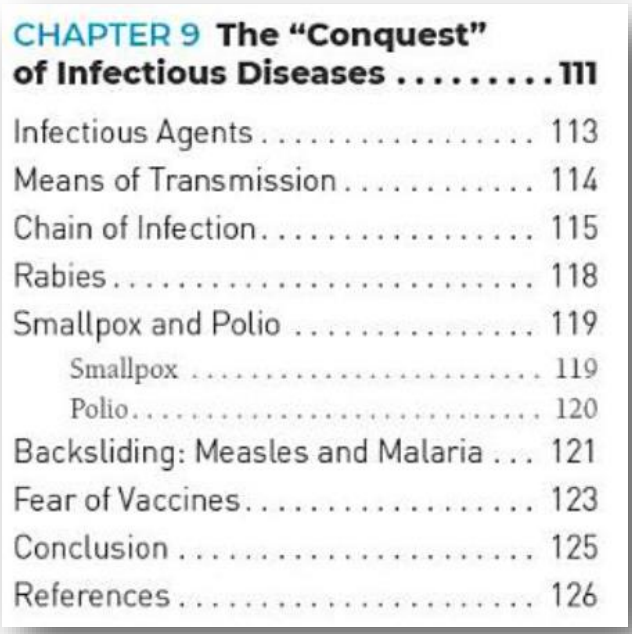
Figure 2: The Chain of Infection

The definition of an infectious agent according to Koch's Postulates is: it must be present in each victim of the disease, it must be possible to isolate it and grow it in a lab, the lab grown culture must cause the disease, and the process must be repeatable.

This leads into a discussion of how each disease can be controlled in various ways, and different interventions, such as managing pooled water or long sleeves, can impact the spread of malaria by mosquitos, while vaccinating dogs and cats is a more cost-effective way to manage the spread of rabies. There is a discussion of fear of vaccines.

CYBERSECURITY PERSPECTIVE

We have no such graph of deaths (or death-equivalents) over time. Our data is sourced from security companies with an interest in being interesting. It lacks precise definitions


CHAPTER 9 The "Conquest" of Infectious Diseases 111
Infectious Agents 113
Means of Transmission 114
Chain of Infection 115
Rabies 118
Smallpox and Polio 119
Smallpox 119
Polio 120
Backsliding: Measles and Malaria . . . 121
Fear of Vaccines 123
Conclusion 125
References 126

Means of transmission is another place where we in cybersecurity generally have it easier. While we frequently fail to capture the break-in, and sometimes important parts are elsewhere, there is no disagreement that some bit of software, either under algorithmic or human control, gets control of a targeted computer or set of computers.

Malware today usually talks to some set of command and control systems. This is another place where we may have an advantage in cybersecurity as an opportunity to intervene in the chain.

Transmission of cybersecurity problems is far less constrained than it is in the physical world.

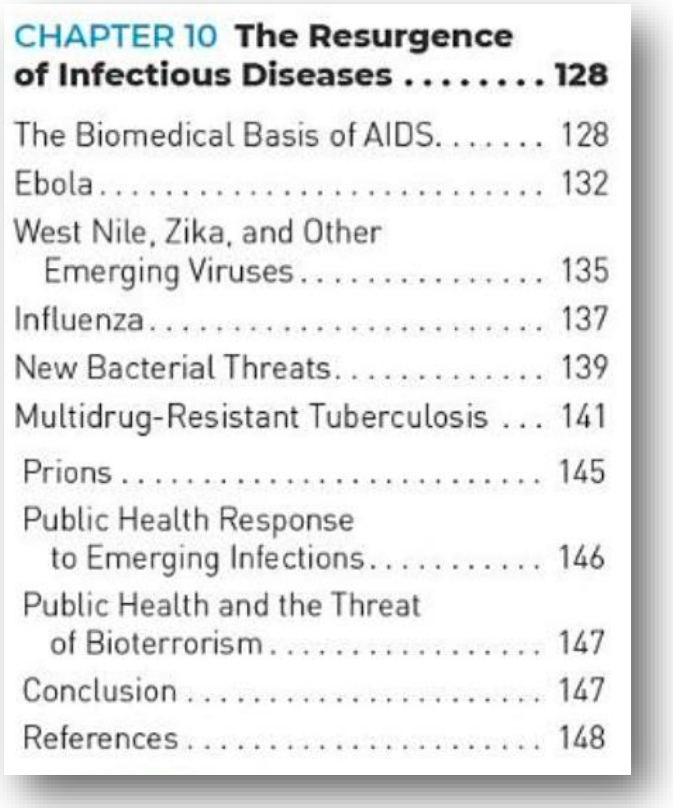
The Chain of Infection is reminiscent of a kill chain. Further, the existence of disease reservoirs outside of observability has an interesting relationship to hidden cybersecurity attacks. Attacks are sometimes hard to detect, and attacker-controlled software can remain undetected for years within an enterprise environment.

It was tempting to write "often hard to detect," but doing so runs into all the problems enumerated elsewhere in this document about base rates and populations.

RESURGENCE OF INFECTIOUS DISEASE (CHAPTER 10)

The chapter begins with a discussion of AIDS, and how it challenged the belief that infectious disease was "under control." The chapter continues with a discussion of Ebola, West Nile, Zika, and influenza, including the emergence of antibiotic resistant strains (which get less attention than I would have expected), prions, and the possibility of bioterrorism.

An interesting aspect of this is how many of the diseases which resurge are those which exist in either domesticated or wild animals and cross over.


CHAPTER 10 The Resurgence of Infectious Diseases 128
The Biomedical Basis of AIDS. 128
Ebola 132
West Nile, Zika, and Other Emerging Viruses 135
Influenza 137
New Bacterial Threats. 139
Multidrug-Resistant Tuberculosis . . . 141
Prions 145
Public Health Response to Emerging Infections. 146
Public Health and the Threat of Bioterrorism 147
Conclusion 147
References 148

CYBERSECURITY PERSPECTIVE

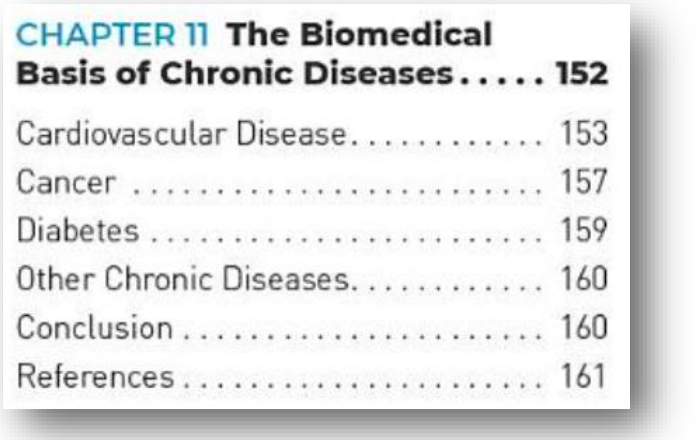
New "strains" of malware emerge, and some re-surge. The nature of computer code makes it easier to make hybrids, or to intentionally change the malware to reduce the efficacy of defenses.

THE BIOMEDICAL BASIS OF CHRONIC DISEASES (CHAPTER 11)

Starting in the 1920s, the success of work against infectious diseases mean that chronic diseases because the leading causes of death in the US. The NIH is the primary body that studies these diseases, with 27 institutes/centers, each dedicated to one chronic disease.

These diseases are studied with a mix of epidemiological and laboratory studies. One crucial tool in lab studies is animal models, which have a mix of effectiveness, cost and ethical concerns associated with them.

There's an extended discussion of atherosclerosis and its relationship to heart disease, and the complexity of advice relating to addressing it, including the advice to avoid cholesterol-heavy foods (now rescinded). There's also discussion of both blood pressure and salt in diets, a discussion of cancer, and a discussion of diabetes.


CHAPTER 11 The Biomedical Basis of Chronic Diseases 152
Cardiovascular Disease 153
Cancer 157
Diabetes 159
Other Chronic Diseases 160
Conclusion 160
References 161

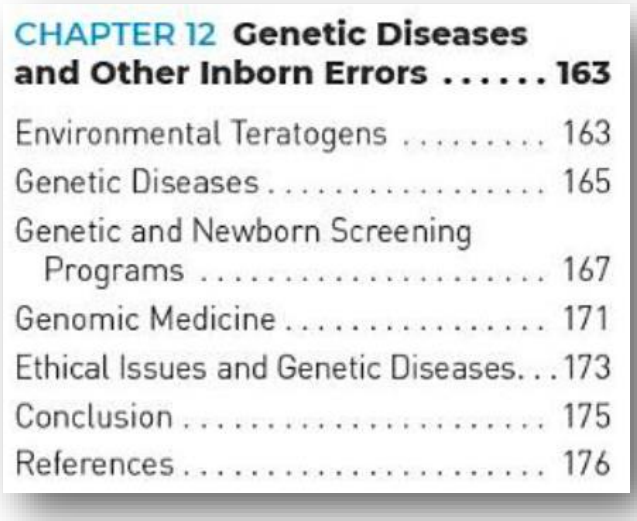
CYBERSECURITY PERSPECTIVE

We do not need to rely on animal models; models of complete "enterprise" systems are harder. Such over-simplification ironically, also impacts on lab models. The relationship between atherosclerosis, cholesterol and heart attacks led to a raft of hard to follow or possibly counter-productive advice, where removing eggs from a diet may have led to less healthy breakfast choices.

Overall, we sadly have few chronic disease equivalents in cybersecurity, because most problems seem to be acute. A reviewer points out this argument is dependent on the definition. My initial response is bad password management is a lifestyle problem, and that is viewing it from the perspective of the consumer. From an enterprise perspective, perhaps getting updates to their computers or managing their employee or customer lost passwords are like a chronic disease. It may be that older devices are the equivalent of aging in people, but aging in software and the random errors that start to happen seems functionally different than cancer, cardiovascular disease or diabetes.

GENETIC DISEASES AND OTHER INBORN ERRORS (CHAPTER 12)

The chapter opens with a discussion of teratogens, environmental agents that cause birth defects. It continues into genetic disease, screening programs for both pre-natal and newborns and then genetic medicine. Genetic medicine has interesting elements of ethics — given that many genes do not lead to disease but rather predispose one to it, is the risk of concern worthwhile? A program to screen African Americans for sickle-cell disease "caused widespread confusion and ill feelings," "many people who were healthy carriers of one gene were discriminated against in school and in employment and were denied health insurance," and "considerable time, effort and money were required to overcome the early mistakes."


CHAPTER 12 Genetic Diseases and Other Inborn Errors 163
Environmental Teratogens 163
Genetic Diseases 165
Genetic and Newborn Screening Programs 167
Genomic Medicine 171
Ethical Issues and Genetic Diseases. . . 173
Conclusion 175
References 176

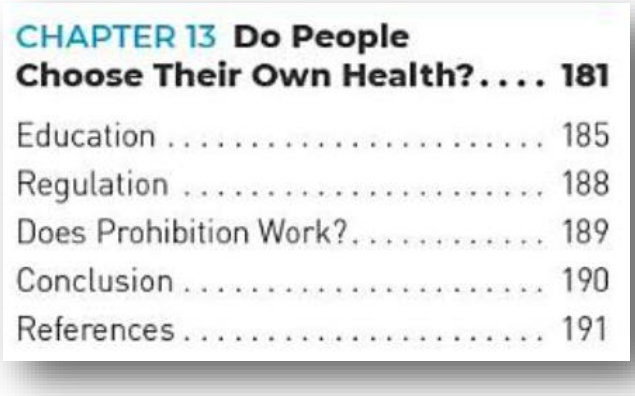
CYBERSECURITY PERSPECTIVE

The issue of early mistakes is likely to be a big one: things like password change requirements and the apparent tension between security and usability are some of the big inhibitors to security practice uptake.

PART IV: SOCIAL AND BEHAVIORAL FACTORS IN HEALTH
DO PEOPLE CHOOSE THEIR OWN HEALTH? (CHAPTER 13)

As we move from infectious disease to chronic ones, the question of cause of death is altered. Is it heart disease, diet or exercise? A team at the CDC crafted a list of "Actual Causes of Death in the United States" (table title from Schneider, not CDC) with the list headed by Tobacco (435,000 deaths in 2000), poor diet and physical inactivity (365,000) with illicit drug use (17,000) as #10. This brings us to the role of educating the public and the relationship between it and regulation, and the question of if (alcohol) prohibition works.

CYBERSECURITY PERSPECTIVE


CHAPTER 13 Do People Choose Their Own Health? 181
Education 185
Regulation 188
Does Prohibition Work? 189
Conclusion 190
References 191

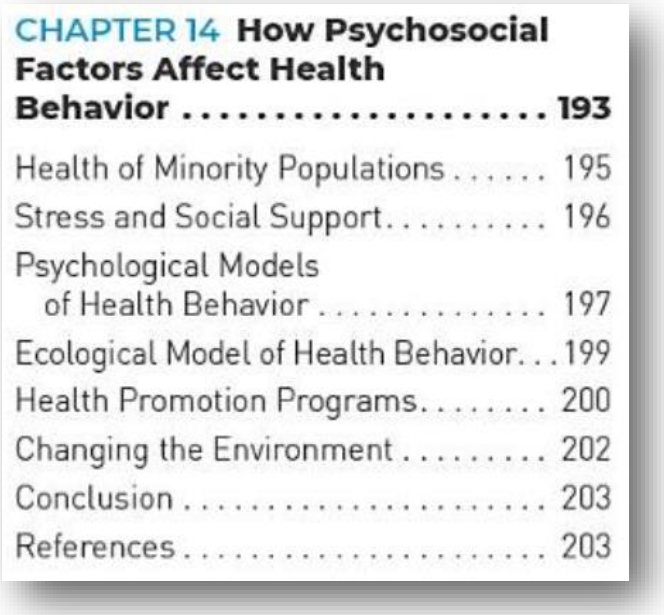
The question of taxonomy and framing (disease of the heart vs tobacco and diet and exercise) are going to be fascinating ones. The latter set are things which simultaneously might be controllable by the person, and carry risks of either victim-blaming or shifting responsibility. For example, we can frame the same issue as a problem of poor user interface design or as people not paying attention. It is certainly in the short to medium term interest of software vendors to shift frames, much like it was in the interest of tobacco companies to talk about freedom and personal responsibilities. I do not mean to imply software and tobacco companies are morally equivalent.

The balance and relationship of education and regulation will be a fruitful one to explore for cybersecurity over time.

HOW PSYCHOSOCIAL FACTORS AFFECT HEALTH BEHAVIOR (CHAPTER 14)

There are diseases that affect different groups differently. Many of these are between countries, but others are within ethnic or religious groups within or across countries, and being married apparently contributes to good health (or not being married reduces it). More, if we only study individuals, we are likely to see individual factors; studying groups allows us to see factors that affect the group. Socio-economic status (SES) is highly correlated with health.

There is discussion of the health of minority populations, stress and social support, and a psychological model of health behavior. That includes the "health belief model," which is a way of assessing how likely someone is to change their behavior based on a health threat. This includes a feeling of vulnerability, the perceived severity of the threat, the perceived barriers to taking action and the perceived effectiveness of taking action. There is also a "transtheoretical model" which envisions change as having 5 stages: precontemplation, contemplation, preparation, action and maintenance. There is an ecological model of public policy, community factors, institutional factors, interpersonal and finally interpersonal factors.


CHAPTER 14 How Psychosocial Factors Affect Health Behavior 193
Health of Minority Populations 195
Stress and Social Support 196
Psychological Models of Health Behavior 197
Ecological Model of Health Behavior ... 199
Health Promotion Programs 200
Changing the Environment 202
Conclusion 203
References 203

All of these inform health promotion programs, such as those to reduce risky sexual behavior to reduce the spread of HIV.

CYBERSECURITY PERSPECTIVE

I moved quickly from thinking this chapter was not relevant to the cyber public health program to the awareness that SES is also correlated with cyber health. For example, being able to replace computers more frequently means those of higher SES are likely to have up to date systems which are more resistant to attack. They can afford consultants or help, and are more likely to know people who work in technology who can help them. They are more likely to be able to afford Apple products which, anecdotally, are more resistant to attack.

Similarly, models like the health belief model or transtheoretic model may helpfully inform efforts to change people's behaviors. They are certainly more nuanced than most which I see in cybersecurity, and almost any which I see outside of academic research.

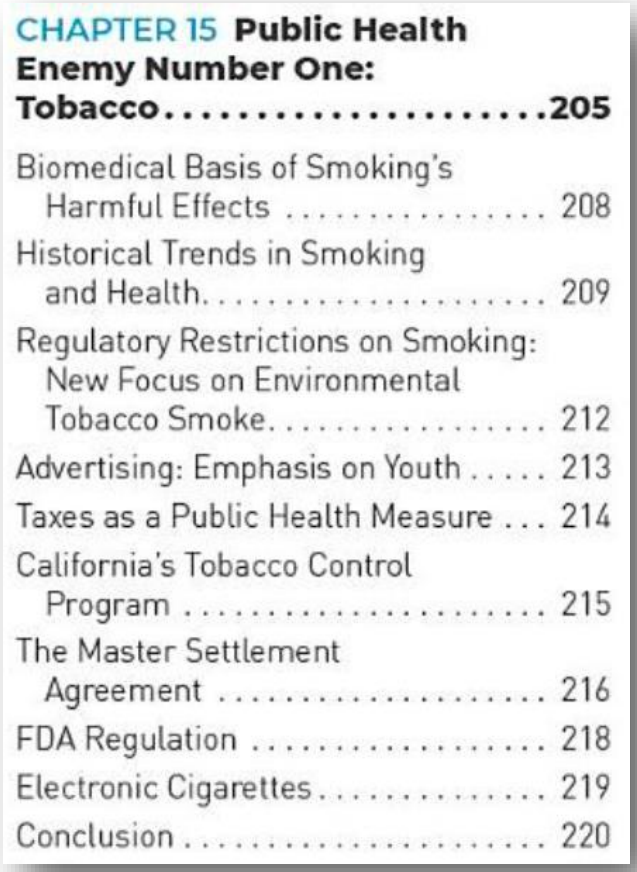
This may be a fruitful area of research, and relates to work in "Folk Models" of computer security done by Rick Wash, as well as research done by Salma et al on why people do not use secure messengers.

PUBLIC HEALTH ENEMY NUMBER ONE: TOBACCO (CHAPTER 15)

Tobacco use kills at least 480,000 and as many as 575,000 people annually. Smokers die ten years earlier than non-smokers, and their mortality rate is nearly 3-fold that of non-smokers.

Tobacco companies marketed their product by giving free cigarettes to soldiers, and then fought hard to manufacture apparent scientific controversy over the dangers of tobacco, and fought regulation even as their products killed millions. (Brandt 2012)

"Public health faces a fundamental dilemma in confronting the current epidemic of tobacco-caused disease: What should be the role of a democratic government in confronting a behavior that is practiced by nearly one in seven adults, and will kill as many of half of them?" Recognition of the addictive nature of tobacco, along with evidence that cigarette companies manipulate levels of tar and nicotine combine with the cost of treating smokers to have slowly shifted responses.

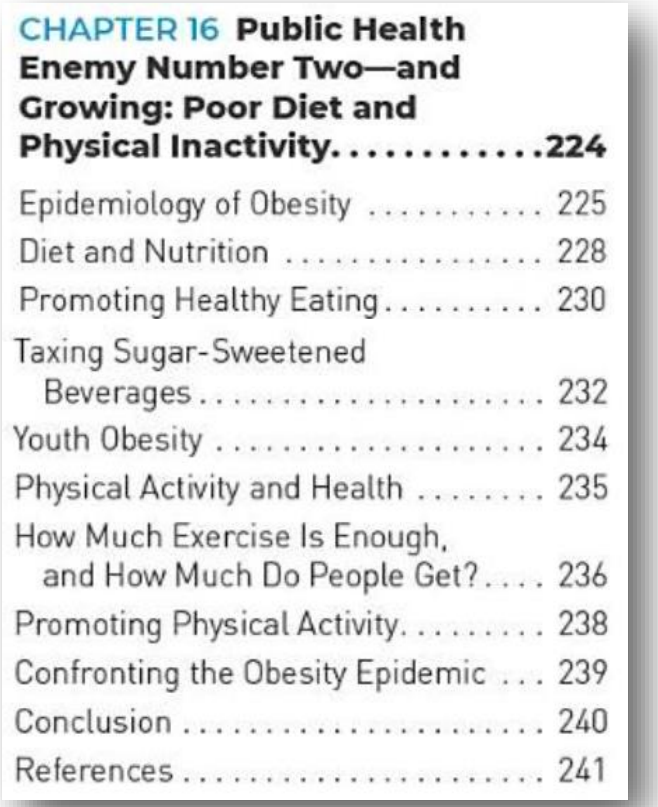

CHAPTER 15 **Public Health Enemy Number One: Tobacco** 205
Biomedical Basis of Smoking's Harmful Effects 208
Historical Trends in Smoking and Health 209
Regulatory Restrictions on Smoking: New Focus on Environmental Tobacco Smoke 212
Advertising: Emphasis on Youth 213
Taxes as a Public Health Measure ... 214
California's Tobacco Control Program 215
The Master Settlement Agreement 216
FDA Regulation 218
Electronic Cigarettes 219
Conclusion 220

CYBERSECURITY PERSPECTIVE

Finally, a chapter with nothing to teach us? The challenge of managing a behavior or tools that attracts some and repulses others is not one with a technical or engineering solution. The role of corporate self-interest in avoiding regulation on tobacco use is fascinating. Companies nominally accepted regulation and limitations and then worked to twist and undermine them. We can see similar dynamics in the regulation of privacy and of online advertising, where companies rolled out wave after wave of tracking technique, and then European regulators put requirements for cookie choice into GDPR. When they did so, we saw advertisers attempting to require people to opt-out cookie by cookie for dozens of cookies, and we saw assertions that intrusive tracking was necessary to operate the product because it was part of the company's business model (rather than the technically necessary intent of GDPR).

PUBLIC HEALTH ENEMY NUMBER TWO (AND GROWING): POOR DIET AND PHYSICAL INACTIVITY (CHAPTER 16)

71.3% of Americans are overweight; 56% of women and 42% of men are trying to lose weight, collectively spending $33 billion dollars per year. The chapter discusses body mass indexes, diet and nutrition, the complexity of promoting healthy eating including when how we eat is so tied to our social interactions, the desire of industries to avoid any message such as "eat less of the stuff we sell," and the reality that taxing sugary drinks is regressive. Similarly, people do not exercise enough, and that has to do with the availability of exercise facilities (including sidewalks).



CHAPTER 16 Public Health Enemy Number Two—and Growing: Poor Diet and Physical Inactivity. 224

Epidemiology of Obesity 225
Diet and Nutrition 228
Promoting Healthy Eating 230
Taxing Sugar-Sweetened Beverages 232
Youth Obesity 234
Physical Activity and Health 235
How Much Exercise Is Enough, and How Much Do People Get? 236
Promoting Physical Activity. 238
Confronting the Obesity Epidemic . . . 239
Conclusion 240
References 241

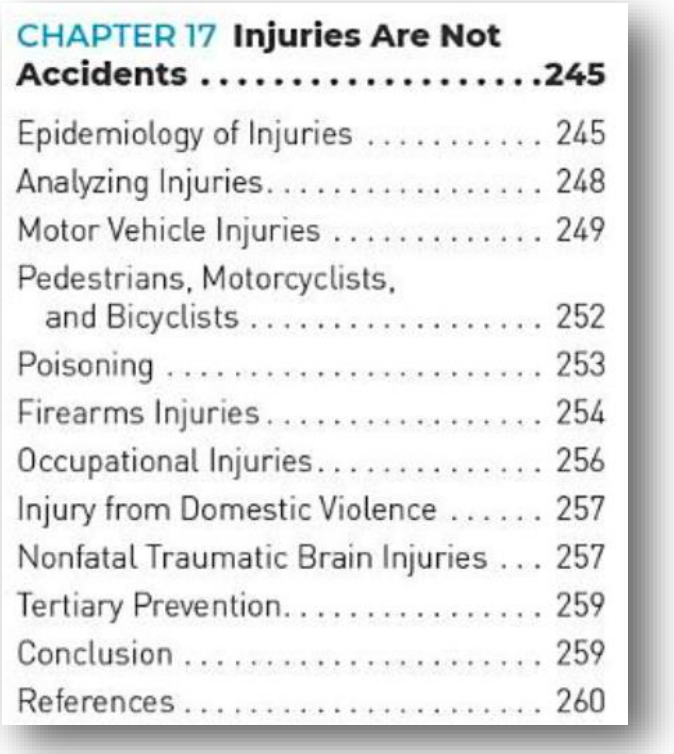
CYBERSECURITY PERSPECTIVE

Almost everyone wants to be thinner and healthier – we all know it is both good for us health-wise and self-esteem-wise. But despite the simplicity of "eat food, mostly plants," it turns out to be hard to achieve that health through better diet. The reality that it is so hard for so many despite these goals should be a useful caution for cyber public health. Perhaps it sets a ceiling on expectations to know that while half of Americans are trying to lose weight, it turns out to be very difficult to lose weight and keep it off. The payoff from that weight loss work is probable years of extra life! Who does not want that? It is probably greater than the payoff for being secure. Or perhaps it is easier to be secure? We do not need to run secure routing protocols to have a nice dinner with friends.

INJURIES ARE NOT ACCIDENTS (CHAPTER 17)

The chapter starts from injuries being the third leading cause of death, the leading cause for people under 50, and one with a high "years of potential life lost." Moreover, recent analysis has resulted in an epidemiological understanding of injuries, and that the frame of who, where, when and how can help us understand and address them. Injuries include unintentional ones (accidental) and intentional (homicide and suicide). Accidental causes start with poison (often narcotics) and motor vehicle, and motor vehicle and firearm deaths are about matched, with each moving substantially in recent years

because of changes in law. We have the best data about deaths, which are recorded more carefully than injuries, especially those injuries that do not result in a hospital admission.


CHAPTER 17 Injuries Are Not Accidents 245
Epidemiology of Injuries 245
Analyzing Injuries..... 248
Motor Vehicle Injuries 249
Pedestrians, Motorcyclists, and Bicyclists 252
Poisoning 253
Firearms Injuries..... 254
Occupational Injuries..... 256
Injury from Domestic Violence 257
Nonfatal Traumatic Brain Injuries ... 257
Tertiary Prevention..... 259
Conclusion 259
References 260

Motor vehicles as a source of injury were spotlighted by Ralph Nader's *Unsafe at Any Speed* in 1966. That book led Congress to create the National Highway Transportation Safety Administration, empowered to collect data on deaths, set safety standards for new cars and to do research on preventing motor vehicle crashes. Alcohol, age, and mobile phone use are all understood to contribute substantially to crashes. Seatbelts have been shown to reduce deaths by 40-50%, and other measures, combined, have caused motor vehicle occupant deaths to fall from 55,000 in 1968 to 37,000 in 2017, despite population growth and growth in miles driven.

Poisoning deaths, largely opioid overdoses, have increased 5-fold over 20 years. Firearm injuries, occupational injuries, and injuries from domestic violence round out the chapter.

AUTHOR'S PERSPECTIVE

Schneider takes an unfortunate perspective on pedestrian deaths, apparently blaming the elderly for walking slowly through poorly engineered environments. She does not touch on the evidence that they are increasing as a result of both distracted drivers and vehicles which are both larger and safer (for the driver), and are thus driven more recklessly (Baker 2019; Gwam 2021). She also discusses the value of bike helmets, ignoring good evidence that bicycle helmet laws reduce cycling and probably have net negative health impacts (de Jong 2012; Roberts 2020).

CYBERSECURITY PERSPECTIVE

Moving our thinking away from "accident" to "predictable event" is a hallmark of safety as a discipline. Safety also teaches us about the importance of looking at the system – if no one wants to get injured on the job, why do they? There are many causes, including a lack of education or awareness and pressure to produce which is at odds with careful operation.

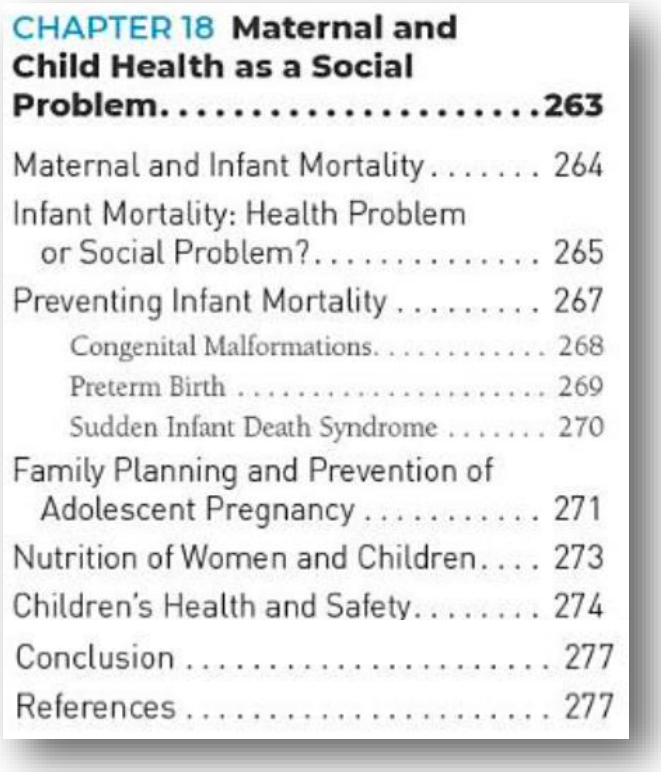
"Identity theft" has not been a focus of this report, but I am prompted by a news story. In it, child identity theft was treated as "just a thing that can happen," rather than a direct result of business practices by credit bureaus and others. The story treated as normal the need for parents to jump

through complex process created by the credit bureaus, and ignored the possibility of public health responses, including regulation.

MATERNAL & CHILDHOOD HEALTH AS A SOCIAL PROBLEM (CHAPTER 18)

Finally, a chapter with nothing to teach us?

There's a lot on maternal and infant mortality and the importance of family planning, nutrition, and early access to vaccines. I was not aware that infant mortality in the US is higher than in most other advanced economies.


CHAPTER 18 **Maternal and Child Health as a Social Problem. 263**
Maternal and Infant Mortality 264
Infant Mortality: Health Problem or Social Problem? 265
Preventing Infant Mortality 267
Congenital Malformations. 268
Preterm Birth 269
Sudden Infant Death Syndrome 270
Family Planning and Prevention of Adolescent Pregnancy 271
Nutrition of Women and Children. . . . 273
Children's Health and Safety. 274
Conclusion 277
References 277

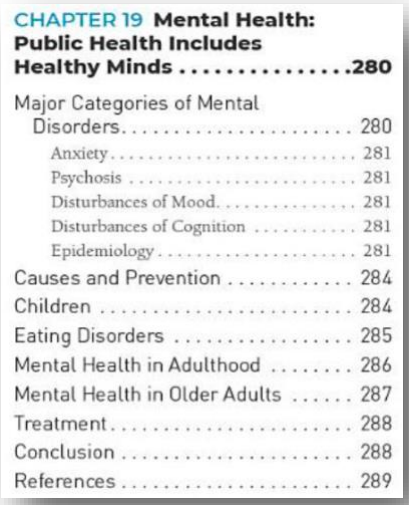
CYBERSECURITY PERSPECTIVE

Nothing to teach us? Apparently not! In the first few pages, we read about the conflict between society's goal of having a healthy population and parental rights to make decisions for their children, possibly extending to what some would see as neglect or abuse. As we think about cybersecurity, the "right to repair" and modify one's own devices, possibly putting either those devices or others at risk has an analogy to parental rights. If I have an unmanaged hobby computer like a Raspberry Pi, it is easy to lose track of it, for updates to break, and for it to be unhealthy for years. It is also easier to just shut off or fix than a child.

MENTAL HEALTH (CHAPTER 19)

Mental health disorders include anxieties, psychosis (issues of perception) and disturbances of mood or cognition. Mental health issues come from both individual factors, family factors, and community factors. There are age specific issues, such as ADHD in children, and there are also eating disorders, typically associated with teens.

This chapter seems to have little relevance to cybersecurity, but the internet has been shown to have impacts on people's mental health, especially on teenage girls who are impacted by sites such as Instagram.


CHAPTER 19 Mental Health: Public Health Includes Healthy Minds 280
Major Categories of Mental Disorders 280
Anxiety 281
Psychosis 281
Disturbances of Mood 281
Disturbances of Cognition 281
Epidemiology 281
Causes and Prevention 284
Children 284
Eating Disorders 285
Mental Health in Adulthood 286
Mental Health in Older Adults 287
Treatment 288
Conclusion 288
References 289

PART V: ENVIRONMENTAL ISSUES IN PUBLIC HEALTH
A CLEAN ENVIRONMENT: THE BASIS OF PUBLIC HEALTH (CHAPTER 20)

The chapter covers the role of government in environmental health, including the identification of hazards, including toxic chemicals (lead, arsenic, asbestos) and radiation. The role of pesticides and environmental chemicals is covered, including bioaccumulation and how workers may be exposed at very high rates and act as "guinea pigs" but that "function" is dispersed because many of the concerning effects take decades to come to pass. The question of 'how safe is safe' and risk-benefit tradeoffs close the chapter.


CHAPTER 20 A Clean Environment: The Basis of Public Health. 293
Role of Government in Environmental Health 294
Identification of Hazards 294
Pesticides and Industrial Chemicals. . . 299
Occupational Exposures: Workers as Guinea Pigs 301
Newer Source of Pollution: Factory Farms. 302
Setting Standards: How Safe Is Safe? . . . 303
Risk–Benefit Analysis 304
Conclusion 305
References 306

There are many stories of unintended consequences or side effects of safety measures, including a program in Bangladesh to replace surface water sources that were teeming with bacteria with safer wells. Unfortunately, it turned out the well water had high levels of arsenic. Another tragic story is that of asbestos. It was installed in all schools built from 1940-1973 as a fire retardant. When its dangers became known, the removal was often done poorly, and many schools did not have the funds to even try to clean it up.

CYBERSECURITY PERSPECTIVE

The environmental effects of cybersecurity problems seem like more of a stretch than the biological ones. There may be an argument that bad security designs lead to increased susceptibility to problems, but it seems to be a stretch.
Fortunately, we have no analog for bio-accumulation, and most individual computers do not stick around for decades, except for the literal toxic wastes in their physical componentry.

CLEAN AIR: IS IT SAFE TO BREATHE? (CHAPTER 21)

Air pollution kills both quickly and slowly. 4,000 deaths are attributed to a weather pattern trapping exhaust and the like in London in 1952, and the long-term effects of air pollution are also troubling. The original 1960s Clean Air Act regulates 6 types of pollutants from whatever source: particulates, sulfur dioxide, carbon monoxide, nitrogen oxides, ozone and lead. There is an ongoing political fight over the cost and benefit of these regulations. 1990 amendments added 180 more, and assigned the EPA to find and regulate the major sources of each.

A 1998 law, the Emergency Planning and Community Right to Know Act (EPCRA) passed in response to the tragedy in Bhopal, requires businesses to disclose their pollution and has resulted in dramatic drops in pollution (by 54% from 1988 to 2001, and another 33% through 2013.)

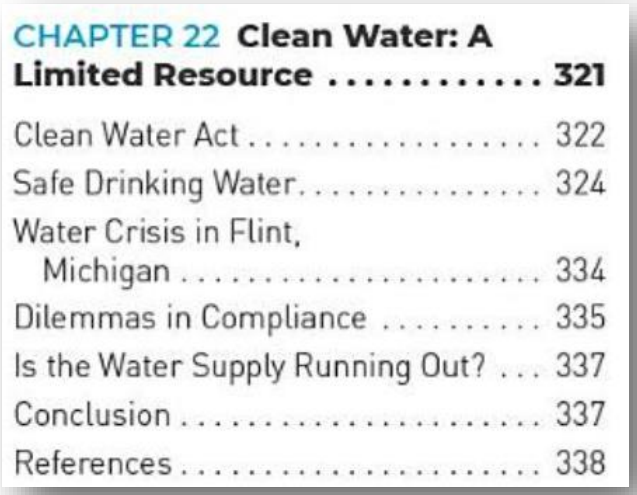
There's a discussion of clean air, and the global effects of air pollution including acid rain, ozone depletion, and global warming.


CHAPTER 21 **Clean Air: Is It Safe to Breathe? 308**
Criteria Air Pollutants 309
Strategies for Meeting Standards.... 311
Indoor Air Quality 314
Global Effects of Air Pollution..... 316
Conclusion 318
References 319

CYBERSECURITY PERSPECTIVE

The impact of the EPCRA in reducing emissions is a thought-provoking one – what are the equivalents of having dangerous chemicals on site? For example, we require breach notification when there's personal information at stake. There's a separate type of problem where an attacker breaks in and puts a second web site on an existing server, and the extra website is a phishing or malware site. Should we require companies to report such issues?

CLEAN WATER: A LIMITED RESOURCE (CHAPTER 22)


CHAPTER 22 **Clean Water: A Limited Resource** **321**
Clean Water Act 322
Safe Drinking Water 324
Water Crisis in Flint, Michigan 334
Dilemmas in Compliance 335
Is the Water Supply Running Out? ... 337
Conclusion 337
References 338

Water quality is now regulated at the national level because water does not respect political boundaries. The Clean Water Act set goals that rivers and lakes should be "fishable" and "swimmable," and eliminated the dumping of pollution into waterways. Over time, it became clear that pollution also came from runoff and the air, and these "non-point" pollution sources are more complex to regulate.

There is an extended discussion of sewage systems and their problems, followed by a discussion of water filtration systems and the many regulated aspects of drinking water, a discussion of the Flint, Michigan disaster, and dilemmas in compliance. Those dilemmas are illustrated by the case of New York City, whose drinking water was deteriorating. A filtration plant would have cost $8B, and New York sought to invest in watershed protection instead. The fights over the right approaches took nearly 20 years.

CYBERSECURITY PERSPECTIVE

The story of how a first law (eliminating the dumping of pollution) was found to not address the problem is likely a story we'll encounter. Apparently obvious fixes — ones that probably improve things — will expose other elements of the problem.

SOLID AND HAZARDOUS WASTE: WHAT TO DO WITH THE GARBAGE? (CHAPTER 23)


CHAPTER 23 **Solid and Hazardous Wastes: What to Do with the Garbage?** **340**
Sanitary Landfills 341
Alternatives to Landfills 342
Hazardous Wastes 343
Coal Ash 347
Conclusion 348
References 348

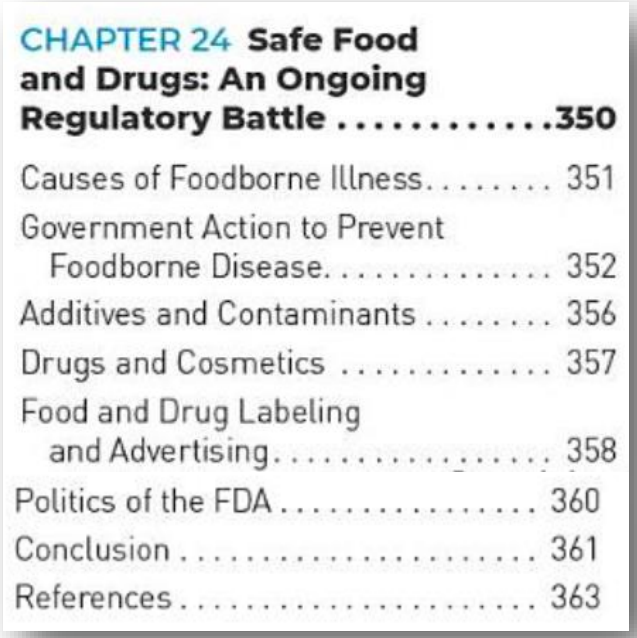
Garbage, as a haven for rats, flies and other vermin has been regulated as far back as ancient Athens. There is both household and industrial garbage, but little apparent relevance to cybersecurity.

SAFE FOOD AND DRUGS: AN ONGOING REGULATORY BATTLE (CHAPTER 24)

Foodborne diseases kill 3,000 Americans each year, and hospitalize 128,000. There is a very complex supply chain involving thousands of meat and poultry plants, tens of thousands of food processing "establishments", hundreds of thousands of restaurants, and the list goes on. The most frequent causes of death are salmonella in poultry or eggs, and e. coli 0157:h7 in ground beef, but also apple juice, lettuce and others. Interestingly these are generally traced back to a point of origin, as are toxins such as botulism or others.

There are a set of practices called Hazard Analysis/Critical Control Points that were designed for astronaut safety in the 1960s, and are a recognizable intellectual antecedent to software threat modeling.[3] There are control measures, particularly irradiating food, that are likely safe but cause consumer backlash, and so less effective processes that leave resides like chlorinating chicken are used, but these also cause trade disputes (see Glotz 2020 for an interesting discussion of the tradeoffs). There are also multiple surveillance systems in place, including Pulsenet, which performs DNA fingerprinting on foodborne bacteria, and Foodnet, which involves outreach to labs, doctors and even surveys of the general public to discover and understand diarrheal illnesses.

All of this is described in a quote from *Safe Food: The Politics of Food Safety* by Marion Nestle: "Today an inventory of food safety activities reveals a system breathtaking in its irrationality." As examples, USDA regulates meat - 20% of the foods - with a $1B budget; FDA regulates the other 80%, also with a $1B budget, and so a frozen cheese pizza facility might be inspected by FDA once a decade, but adding pepperoni and bringing it under USDA might lead to daily inspections. There are complex political factors, including the motivations of companies and people's desire to select 'natural' medicine, etc. The politics of drugs (also regulated by the FDA) are more complex, with companies banned from selling new drugs without approval, and patients with life threatening conditions unable to try drugs which might save them because of the risks of side effects.


CHAPTER 24 **Safe Food and Drugs: An Ongoing Regulatory Battle 350**
Causes of Foodborne Illness. 351
Government Action to Prevent Foodborne Disease. 352
Additives and Contaminants 356
Drugs and Cosmetics 357
Food and Drug Labeling and Advertising. 358
Politics of the FDA 360
Conclusion 361
References 363

Lastly, in the news today, "The US government's tyrannical reign over a classic condiment is finally ending." The final rulemaking, which occupies a full four pages of the Federal Register, revokes the "standard of identity for French dressing" after a 22-year effort by the trade group The Association for Dressings and Sauces (FDA 2022).

CYBERSECURITY PERSPECTIVE

First, I am jealous of the determination to trace outbreaks to a root cause, along with the multiple networks for passive and active detection of problems (Pulsenet and Foodnet). That jealousy is modulated by the complexity of regulation, the irrationality of the systems that have evolved, and the questions about the results.

I am less jealous of a regulatory system in which changing a rule about French dressing takes 22 years.

[3] The steps are: 1. Perform a hazard analysis; 2. Determine control points; 3. Determine critical limits; 4, 5, 6. Establish monitoring processes, corrective actions, and verification processes. 7. Establish record keeping and documentation.

There is a very complex relationship between regulation and security. Regulations such as the Wassenaar Arrangement on export controls have a complex relationship with freedom of speech and software. Similarly, regulations such as those that forbid browsing "pornography" may cause people to install insecure software to bypass those regulations, and leave their system at higher risk.

Lastly, a personal story about judgement. I was exceptionally skeptical of Bluetooth as an addition to insulin monitors. I focused on the cybersecurity problems until a meeting I was in was interrupted by an alert on someone's phone, letting them know that their blood sugar was dangerously imbalanced. It is easy to deride interest groups or dismiss the politics that surround French dressing, and harder to design systems without these issues.


CHAPTER 25 **Population: The Ultimate Environmental Health Issue 365**
Public Health and Population Growth 367
Global Impact of Population Growth: Depletion of Resources . . . 369
Global Impact of Population Growth: Climate Change 371
Dire Predictions and Fragile Hope . . . 375
Conclusion 376
References 377

POPULATION: THE ULTIMATE ENVIRONMENTAL HEALTH ISSUE (CHAPTER 25)

This chapter covers population growth, including the idea of carrying capacity, how public health has contributed to population growth by driving down early childhood deaths globally, resource depletion concerns, and global warming. There seems to be relatively few lessons for cybersecurity.

PART VI: MEDICAL CARE AND PUBLIC HEALTH
IS THE MEDICAL CARE SYSTEM A PUBLIC HEALTH ISSUE (CHAPTER 26)

This chapter is focused on the relationship between public health and medicine, how each is funded, and the associated tensions. The tone is set at the start "Vastly greater sums are spent each year on medical care than on public health measures aimed at preventing disease and disability. Is that a rational allocation of resources?" The chapter discusses how medical bills are paid, how they're rising rapidly, the narrow cases of a right to medical care, and the social insurance programs which exist in the US.


CHAPTER 26 **Is the Medical Care System a Public Health Issue? 383**
When Medical Care Is a Public Health Responsibility 384
The Conflict Between Public Health and the Medical Profession 385
Licensing and Regulation 388
Ethical and Legal Issues in Medical Care 389
Ethical Issues in Medical Resource Allocation 391
Conclusion 393
References 394

CYBERSECURITY PERSPECTIVE

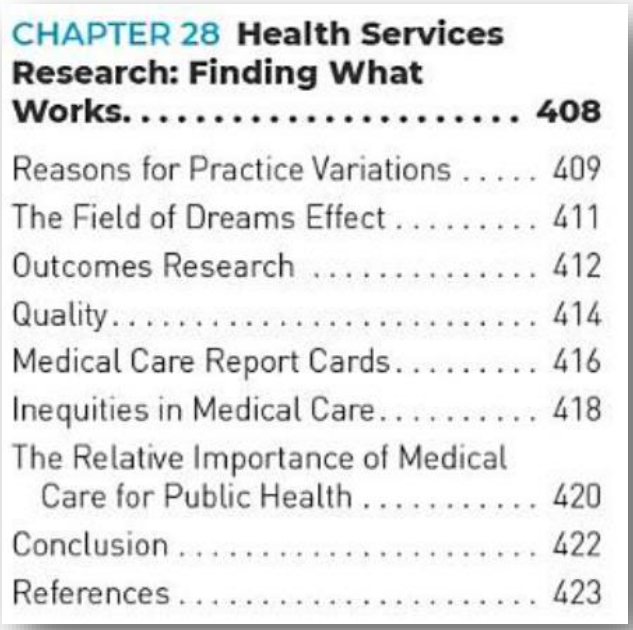
Although the chapter nominally has little to say to cybersecurity, there is an interesting question raised by payment: should the government pay for some forms of assistance (insurance) for the poor, to help them clean up their computers, and stop those from being reservoirs of disease? How this might work, if the cybersecurity ("medical") firms might oppose it, etc. are all possible future questions.

WHY THE US MEDICAL SYSTEM NEEDS REFORM (CHAPTER 27)


CHAPTER 27 Why the U.S. Medical System Needs Reform. 395
Problems with Access 396
Why Do Costs Keep Rising? 399
Approaches to Controlling Medical Costs 400
Managed Care and Beyond 401
The Patient Protection and Affordable Care Act 403
Rationing 404
Conclusion 405
References 406

The chapter opens with damning numbers on the growth of medical spending, and that US spending is the highest in the world for some of the worst outcomes (amongst comparable countries). It enumerates problems with access, and a variety of other issues.

HEALTH SERVICES RESEARCH: FINDING WHAT WORKS (CHAPTER 28)


CHAPTER 28 Health Services Research: Finding What Works. 408
Reasons for Practice Variations 409
The Field of Dreams Effect 411
Outcomes Research 412
Quality 414
Medical Care Report Cards 416
Inequities in Medical Care 418
The Relative Importance of Medical Care for Public Health 420
Conclusion 422
References 423

The chapter opens with a discussion of how two towns in Vermont had radically different rates of tonsil removal (8% vs 70%), and how such "small-area analyses" of rates of treatments regularly find large disparities which are not easily explained. These variations are higher for conditions there's disagreement about the appropriate treatment, but they often result from "practice style" differences which are not supported by evidence one way or another. There is a complex relationship between availability of care and outcomes. In the 1980s, researchers found that Boston had 4.5 beds per thousand residents, while New Haven only had 2.9, but somehow mortality rates and other measures of quality of care were about the same. It seems likely that hospitalization was thus either over-used in Boston or underused in New Haven. Which is hard to determine.

This leads to a discipline of outcomes research, where cohorts are followed to enable analysis of treatment differences. For example, one study looked at prostate removal, a treatment that was done for 60% of men by age 80 in some places, and 20% in other places. The surgery did not increase life expectancy, and had mixed effects on quality of life. "The results of these studies indicate a need for better informing patients about their choices and the probable outcomes…"

This complexity led Congress to create an Agency for Healthcare Policy and Research, which started by looking at lower back pain. Lower back pain treatments cost roughly $80B in 2011, and surgical rates are 3-fold different across the country. The agency recommended that lower-risk treatments be the norm. Quoting: "Back surgeons responded with both rage and political action." The successor Agency for Healthcare Research and Quality (AHRQ) no longer develops guidelines, but maintains a clearinghouse of guidelines written by others.

There is an extended discussion of quality of care, the importance of medical errors as a cause of death, and the value of routine records collection as a tool for learning, and the importance of

inequities in medical care. These are followed by another analysis of the causes of early death. This one rates behavioral patterns at 40%, genetic pre-disposition at 30%, social circumstances at 15% and medical error at 10%. The alert reader will note that this is the 3rd or 4th taxonomy of causes of death, and perhaps, like me, ask why the public health folks cannot pick just one. A moment's reflection allows us to remember that people and society are both complex, and the many ways to slice the data are a strength, not a weakness.

That discussion of the quality of care is followed by a discussion of 'The relative importance of medical care for public health,' which points out that if we were to allocate money to improving overall health outcomes, either as individuals or a society, we could do a lot better. At the societal level, spending on education, housing and environment has dramatic payoffs, and similarly, investments on a personal level into healthy lifestyle pay off better than investments in acute care.

CYBERSECURITY PERSPECTIVE

While availability of security services is likely less geographically dependent than medical care, selection of controls may be dependent on factors like industry. For example, integrations of various defensive technology with say, dental or legal practice software may lead to dramatically different rates of either those technologies, or specific implementations of the technologies.

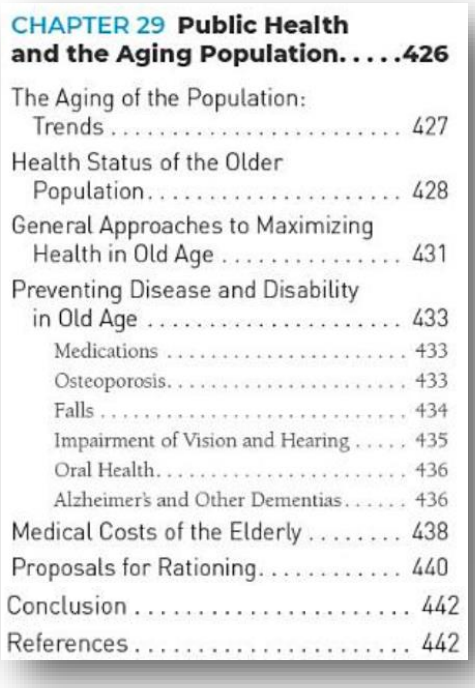
The prostate example is interesting because it argues for variation of treatment based on personal choices. In the cybersecurity realm, this is often glommed into a "risk analysis" and "what is right for your business," which are criteria applied to almost every control. In medicine, the right treatments are sometimes known, or debated, and the most common conditions have well-understood AHRQ-gathered treatment guidelines. Compare and contrast to phishing or ransomware.

For phishing, our guidance is very much influenced by a perception of what is possible: architectures which keep mail clients as local "thick" clients like Outlook or Mail.app, with the feature of directly invoking other complex clients (Word, Excel, Java, Flash) are inherently more at risk from attachment-driven phishing than those which run entirely in the cloud and browsers. How much more at risk? What is the outcome of shifting that? Is it worthwhile? It is easy to make the intellectual argument that those thick clients are riskier, but how much riskier are they? We do not know.

The question of "are we spending well in cybersecurity" may have an analogous argument about resource allocation: it may be that investments in a free operating system that does not run in C, maintenance and security support for popular open source libraries, work on infrastructural capabilities such as unified logging formats, or others could have a dramatic effect on overall rates of problems. The list here is intended to be illustrative, not definitive. Again, evidence on outcomes with robust analyses of contributing factors could enable a much more robust conversation.

PUBLIC HEALTH AND THE AGING POPULATION (CHAPTER 29)

The chapter illustrates how more people are living longer and healthier, and the complex economic problems as they need more care as they age. Few apparent lessons for cybersecurity, especially as there's no outrage at pulling the plug from an aging computer.

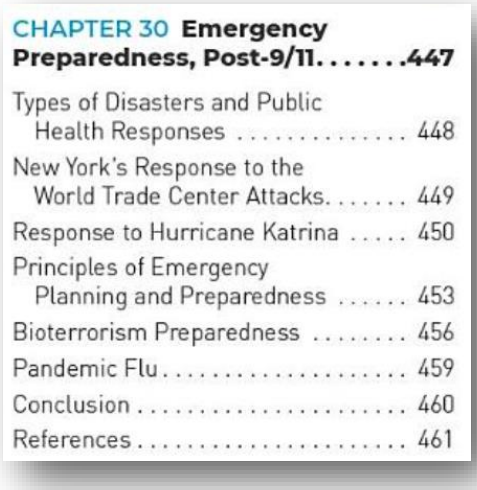

CHAPTER 29 **Public Health and the Aging Population. 426**
The Aging of the Population: Trends 427
Health Status of the Older Population 428
General Approaches to Maximizing Health in Old Age 431
Preventing Disease and Disability in Old Age 433
Medications 433
Osteoporosis. 433
Falls 434
Impairment of Vision and Hearing 435
Oral Health. 436
Alzheimer's and Other Dementias. 436
Medical Costs of the Elderly 438
Proposals for Rationing. 440
Conclusion 442
References 442

CYBERSECURITY PERSPECTIVE ON PART VI

The CyberGreen Internet Infrastructure Health Metrics Framework program used a rubric of "harm to self/harm to others" to select what to measure. A lesson from this book analysis project is that public health measures the health of a population – the things that we might consider as harms to self, and that raises the question of if a cyber public health project should attempt to measure population health.

PART VII: THE FUTURE OF PUBLIC HEALTH EMERGENCY PREPAREDNESS, POST 9/11 (CHAPTER 30)

Emergency preparedness includes planning, preparation and drills. There's discussion of both 9/11 and Hurricane Katrina, the threat of bioterrorism and a short section on pandemic flu.


CHAPTER 30 **Emergency Preparedness, Post-9/11. . . . . .447**
Types of Disasters and Public Health Responses 448
New York's Response to the World Trade Center Attacks. 449
Response to Hurricane Katrina 450
Principles of Emergency Planning and Preparedness 453
Bioterrorism Preparedness 456
Pandemic Flu. 459
Conclusion 460
References 461

CYBERSECURITY PERSPECTIVE

We have CERTS – Computer Emergency Response Centers, but response is but one aspect of overall preparedness. Most CERTs do not run big simulations or war games, but the US government has done a few, with names like "Cyber Storm."

The apparently never-ending stream of crises, which last month included log4j and this month includes preparation for cyber- and physical- war in Ukraine leaves relatively little bandwidth for more strategic initiatives. There is also a "Cyber Readiness Index" which may be relevant.[4]

[4] https://www.potomacinstitute.org/academic-centers/cyber-readiness-index

PUBLIC HEALTH IN THE 21ST CENTURY: ACHIEVEMENTS AND CHALLENGES (CHAPTER 31)

In the 20th century, average lifespans rose from 47 to 77, largely as a result of public health strategies. The achievements include vaccination, vehicle safety, safer workplaces, infectious disease control, safer food and water (including fluoridation), and a recognition of the dangers of tobacco.

There is a strategic planning process across the government, initiated by a 1990 Surgeon General report titled "Healthy People", and now a regular decade long planning and measurement process at healthypeople.gov, using a technique of setting objectives and measuring progress against them.

There's roughly a two-page table of leading health indicators with metrics, ranging from air quality index to infant deaths, to adult aerobic activity or cigarette smoking. Each has its progress measured in start of decade, end of decade numbers.

There are challenges related to the integration of medicine and public health, and the rapid growth of connectivity enables a great many things, while the HIPAA privacy rules inhibit a few.


CHAPTER 31 **Public Health in the Twenty-First Century: Achievements and Challenges 463**

Challenges for the 21st Century 464
Strategic Planning for Public Health . . . 466
Dashed Hopes for the Integration of Public Health and Medical Practice 470
Information Technology 471
The Challenge of Biotechnology 473
The Ultimate Challenge to Public Health in the 21st Century 474
Conclusion 474
References 475

CYBERSECURITY PERSPECTIVE

The complexity of securing computers was clear in the 1960s and 70s, before they were interconnected. Their complete interconnection has brought tremendous benefits, and some very real challenges.

The strategic planning activity is a fascinating challenge. What dozen measures could we take and manage towards, that would give us a similar impression of the overall health of the technology in our world? Perhaps a first step would be the establishment of a group to ask that question.

3. CONCLUSION

Where should we go from here?

Having done this work, I am increasingly optimistic that a public health model will be a useful frame.

There is a need for proof that the model is helpful, and that requires either a crisper definition, or comfort that we have a set of related, overlapping goals. I believe that imprecision is ok. A reviewer in actual public health commented that this paper does not discuss the concept of global burden of disease, and I'm sure others in that field will draw other issues to our attention.

As our lives are increasingly intertwined with technology, issues such as mental health are impacted by the engagement algorithms used by social media sites, and public acceptance of vaccines is being challenged in ways promoted by those algorithms. So public health is impacted fairly directly by technology.

The ways in which enterprises, small businesses and individuals select, use, manage, maintain and retire technology all have impact on the security, comfort and well-being of the people whose lives or data are tied into those systems, and the ways in which we think about the security of those systems remains nascent.

We can and learn from public health to create a discipline of cyber public health.

REFERENCES

Abu-Salma, Ruba, M. A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina and M. Smith, "Obstacles to the Adoption of Secure Communication Tools," 2017 IEEE Symposium on Security and Privacy (SP), 2017, pp. 137-153, doi: 10.1109/SP.2017.65

Baker, Peter C. "Collision Course: Why Are Cars Killing More and More Pedestrians?" *The Guardian*, October 3, 2019. https://www.theguardian.com/technology/2019/oct/03/collision-course-pedestrian-deaths-rising-driverless-cars.

Brandt, Allan M. "Inventing Conflicts of Interest: A History of Tobacco Industry Tactics." *American Journal of Public Health* 102, no. 1 (2012): 63–71. https://doi.org/10.2105/ajph.2011.300292.

Cantor, Matthew. "Libération! Long-Derided French Dressing Freed from Strict US Rules." *The Guardian*, January 14, 2022. https://www.theguardian.com/food/2022/jan/14/french-dressing-fda-rules.

de Jong, Piet. "The Health Impact of Mandatory Bicycle Helmet Laws." *Risk Analysis* 32, no. 5 (2012): 782–90. https://doi.org/10.1111/j.1539-6924.2011.01785.x.

FDA. "French Dressing; Revocation of a Standard of Identity." Federal Register. Food and Drug Administration, January 13, 2022. https://www.federalregister.gov/documents/2022/01/13/2022-00494/french-dressing-revocation-of-a-standard-of-identity.

"Framingham Study." Boston Medical Center. Accessed December 27, 2021. https://www.bmc.org/stroke-and-cerebrovascular-center/research/framingham-study.

Gatlan, Sergiu. "FBI: Hackers Use Badusb to Target Defense Firms with Ransomware." BleepingComputer. BleepingComputer, January 11, 2022. https://www.bleepingcomputer.com/news/security/fbi-hackers-use-badusb-to-target-defense-firms-with-ransomware/.

Glotz, Julia. "Chlorinated Chicken Explained: Why Do the Americans Treat Their Poultry with Chlorine?" The Grocer. The Grocer, August 3, 2020. https://www.thegrocer.co.uk/food-safety/chlorinated-chicken-explained-why-do-the-americans-treat-their-poultry-with-chlorine/555618.article.

Gwam, Peace. "More and More American Pedestrians Are Dying Because of Larger Vehicles. Incorporating Data in Safety Regulations Can Help." Urban Institute, October 19, 2021. https://www.urban.org/urban-wire/more-and-more-american-pedestrians-are-dying-because-larger-vehicles-incorporating-data-safety-regulations-can-help.

Hay, Mark. "Everything You Know about Cheese Is a Lie." The Outline, January 18, 2018. https://theoutline.com/post/2980/raw-cheese-regulation-usa-history.

IoT Analytics. *Total Number of Device Connections (Incl. Non-IoT)* . November 2020. *IoT Analytics*. https://iot-analytics.com/wp/wp-content/uploads/2020/11/IoT-connections-total-number-of-device-connections-min.png .

Lyngaas, Sean. "FBI Warns Cybercriminals Have Tried to Hack US Firms by Mailing Malicious USB Drives." CNN, January 7, 2022. https://www.cnn.com/2022/01/07/politics/fbi-usb-hackers-warning/index.html.

Maayan, Gilad David. "The IOT Rundown for 2020: Stats, Risks, and Solutions." Security Today, January 13, 2020. https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx.

Myhrvold, Nathan, and Chris Young. "Cooking Pork Safely: The Science." The Guardian. Guardian News and Media, May 26, 2011. https://www.theguardian.com/lifeandstyle/2011/may/26/cooking-pork-safely-the-science.

Osterman Research. *Why Zero Trust Is Important*. Symmetry Systems, November 2021. https://f.hubspotusercontent40.net/hubfs/7473991/Gated%20Content/Osterman%20Research%20-%20Why%20Zero%20Trust%20is%20Important.pdf.

Roberts, Jessica, Caron Whitaker, Gersh Kuntzman, Angie Schmitt, and Stephen Miller. "Bike Group to Feds: Helmet Laws Are Bad." Streetsblog USA, January 17, 2020. https://usa.streetsblog.org/2020/01/17/bike-group-to-feds-helmet-laws-are-bad/.

Rostron, Allen. "The Dickey Amendment on Federal Funding for Research on Gun Violence: A Legal Dissection." *American Journal of Public Health* 108, no. 7 (July 2018): 865–67. https://doi.org/10.2105/ajph.2018.304450.

Vailshery, Lionel Sujay. "IOT Connected Devices Worldwide 2019-2030." Statista, March 17, 2022. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.

Li W, Onyebeke C, Huynh M, Castro A, Falci L, Gurung S, Kennedy J, Maduro G, Sun Y, and Van Wye G. Summary of Vital Statistics, 2017. New York, NY: New York City Department of Health and Mental Hygiene, Bureau of Vital Statistics, 2019. https://www1.nyc.gov/assets/doh/downloads/pdf/vs/2017sum.pdf

Sedenberg, Elaine M., and Deirdre K. Mulligan. "Public Health as a model for cybersecurity information sharing." Berkeley Tech. LJ 30 (2015): 1687.

Wash, Rick. "Folk models of home computer security." Proceedings of the Sixth Symposium on Usable Privacy and Security. 2010.

ACKNOWLEDGEMENTS

This report was written by Adam Shostack for the CyberGreen Institute.

We would like to acknowledge helpful comments and discussion from Abie Flaxman, Dan Geer, Kurtis Heimerl, Shawn Hernan, Yurie Ito, Sudheesh Singanamalla and Arastoo Taslim.