Is a Public Health Framework the Cure for Cyber Security?

Brent Rowe, RTI International
Michael Halpern, RTI International
Tony Lentz, RTI International

Abstract. The public health community has developed robust systems for objectively identifying and studying health threats and coordinating interventions, whereas the cyber security community is still relatively immature in its use of an objective, systematic approach. In this paper, we present a detailed public health framework—including descriptions of public health threats encountered and interventions used—and develop parallels between public health and cyber security threats and interventions. We propose that employing a public health framework to understand individual risk preferences for cyber security can identify the types of interventions and related implementation and communication strategies that will more effectively improve cyber security.

Section 1: Introduction

A significant and growing component of U.S. and worldwide cyber security is the relative insecurity of individual Internet users—the threat that some individuals pose to themselves or others through their vulnerability to cyber attack. Cyber threats are difficult to identify and are often poorly understood by users, which may leave them more vulnerable to attacks than they would otherwise perceive. Moreover, the anonymous and dispersed nature of today's cyber threats have proven that these threats are particularly difficult to target for preventative intervention. As the number of worldwide Internet users approaches 2 billion, the scale of affected individuals shows no sign of slowing.

Although a variety of distributed methods have been used to incrementally improve the cyber security of individuals and businesses, a new broad strategic framework may be needed. In the past, organizations and individuals have been marketed to by cyber security companies such as McAfee and Symantec. More recently, a diverse and growing number of software, hardware, and service providers advertise offers to improve cyber security. No centralized approach has been successfully used to coordinate action; the government has played a relatively limited role, developing standards for industry and, more recently, distributing educational materials online and through presentations to schools and civic organizations. At present, regulation is being considered as a way to increase widespread action, with most of the focus on business security.

In light of the complexities of cyber security, the field of public health offers a framework that may help to focus and improve cyber security research and the selection of intervention strategies. Cyber security threats, like public health threats, often pose a risk not only to the targeted or infected individuals but also to others who are at risk of secondary exposures to a contagion. Recently, members of the private sector, public sector, and the research community have begun to discuss the benefits of this new paradigm [1, 2, 3].[1]

Over the years, the public health community has had many successes [4] that may offer models for understanding and addressing cyber security. Much of public health focuses on identifying and monitoring threats, preventing illnesses or injuries before they occur, and diagnosing conditions in early stages when they are most easily treated and cured. Cyber security threats can similarly be addressed by seeking to prevent successful attacks or stopping the spread of threats at various stages of proliferation.

In this paper, we present a public health framework that can be used to identify and describe specific cyber security threats and potential solutions. We then focus on specific ways in which public health research may inform cyber security research by asking the question: how can the established body of public health research be leveraged to assess cyber security risk perceptions, an area of identified need in the cyber security community?[2] A copious amount of research has investigated individuals' risk perceptions regarding the threat and spread of infectious disease and the factors that may influence an individual to engage in activities to prevent disease transmission. We propose that research is needed that seeks to identify types of cyber security interventions—modeled on public health successes—that would be effective in increasing cyber security, based on individual risk preference estimates. Public health successes would be used to select potential cyber security solutions, and models for understanding demand for specific cyber security solutions would be developed based on public health models of risk preference. By improving understanding of cyber security risk preferences, cyber security researchers, and the cyber security industry would be better able to develop and promote products that more effectively and efficiently improve cyber security.

Section 2: Past Research

The cyber security community has yet to identify a suitable framework through which both the private and public sectors can together effectively combat threats to the cyber security of individuals and businesses. Several past research efforts have sought to explore definitions of the threats or to identify potential solutions by using a public health framework [5]. Of particular importance to cyber security coordination is developing an understanding of risk preferences, and the public health community offers many lessons.

Previous papers and research that have looked to the public health domain for lessons on cyber security have focused on identifying the core concepts and practices that could be adopted to promote better "cyber health." In a 2010 white paper published by Microsoft, Scott Carney, Corporate Vice President of Trustworthy Computing, suggested that stakeholders concerned about addressing cyber threats should support practices modeled on efforts to address human illness; moreover, he proposed that cyber security efforts modeled on public health techniques ranging from the simple to the systematic should be adopted. Charney [2] promotes a security approach centered on device health. He lays out two complementary approaches to advancing device health: (1) bolstering efforts to identify infected devices and (2) promoting efforts to better demonstrate device health. Ultimately, this approach would result in devices presenting a "health certificate" that demonstrates the current state of health of the device, which would allow other devices to take a series of actions based on the information contained in the health certificate.

Another recent white paper, issued by IBM [6] argues for cyber security and IT specialists to move away from "military or security metaphors commonly used" and to embrace a new perspective based on the public health and safety model. The paper's authors suggest that the current cyber security paradigm is too rigid and not flexible enough to meet the day-to-day challenges cyber threats present. Instead, the cyber security problem should be addressed in a "flexible, inclusive, and coordinated manner" for which the public health and safety model is well suited to provide and has demonstrated success in doing. The public health and safety model approach to cyber security should focus not only on detection and prevention of threats, but also on "risk-management, coordination, and communication among a broad range of stakeholders." As others have suggested [3] adopting a public health and safety approach could allow for the cyber security problem to be viewed as part of an ecosystem, where problems are constantly evolving.

The most comprehensive view of adopting public health as a model for cyber security has been advanced by Mulligan and Schneider [1]. Mulligan and Schneider argue that cyber security is a public good and any future doctrines of cyber security should recognize the parallels between public health and cyber security as public goods and develop strategies based on this idea.

Section 3: Lessons From Public Health

Definition of Public Health

To consider how public health may serve as a model for cyber security activities, it is necessary to first define the term public health and understand the activities or components that are part of this discipline. In the 1988 Institute of Medicine report The Future of Public Health, public health is defined as "what we, as a society, do collectively to assure the conditions in which people can be healthy" [7]. A somewhat expanded definition of public health is "the science and art of protecting and improving the health of communities through education, promotion of healthy lifestyles, and research for disease and injury prevention."[3] A key element in both of these definitions is that public health refers to the health of communities or populations. Clearly, communities are made up of individuals, and many public health activities involve addressing health issues at the individual level. However, the main distinction of public health as opposed to other types of health care is that public health focuses on the health of groups of people rather than on one person at a time. In addition, although individuals need medical care only at certain times, communities need public health all the time to stay healthy.[4]

A Classification Framework Based on Categories of Public Health Threats

As a starting point for the use of public health activities as a framework for considering cyber security activities, it may be most appropriate to consider the major categories or types of public health "threats," that is, diseases, health impairments, and health risks targeted by public health professionals. We developed the following framework based on a review of various public health classification systems and consideration of the types of threats that are the focus of most public health activities. Further, this framework was conceived with the objective of showing parallels between public health and cyber security; that is, our plan was to present public health threats in a context that would allow for a similar or related classification system for cyber security threats.[5] In our classification framework, public health activities directed at specific categories of threats include the following:

1. Communicable diseases. These threats include illnesses that are directly spread between individuals or can be transmitted between individuals by a nonhuman vector (e.g., spread of malaria by mosquitoes). Examples of public health activities addressing this class of threats include vaccinations, screening and treatment for tuberculosis and sexually transmitted diseases, control of vectors that can spread communicable diseases (e.g., mosquito control), and potential quarantine of individuals who can transmit diseases.

2. Noncommunicable diseases. These include conditions that are not directly spread among people, such as coronary artery disease, cancer, diabetes, arthritis, and chronic obstructive pulmonary diseases. An important characteristics of many noncommunicable diseases is that they may begin as asymptomatic conditions, either undetectable or detectable only by specialized screening tests, and over moderate to long periods of time can develop into lifelong conditions that can severely affect quality of life and survival. Precursors that increase risk for the development of noncommunicable diseases may include communicable diseases; for example, certain strains of human papillomavirus, a communicable agent, can increase the risk of development of cervical cancer. The goals of public health activities related to noncommunicable disease threats are to prevent development of these conditions (through preventing the development of/exposure to risk factors or identifying and treating risk factors prior to disease development), identify conditions early in the course of the disease when they have had limited effects and are more easily treated, and stop further progression of conditions once they have fully developed.

3. Risk behaviors. As a type of public health threat, risk behaviors are not fully separate from communicable or noncommunicable diseases; many risk behaviors can lead to the development of such diseases.[6] However, risk behaviors may be thought of as a separate public health threat because the public health activities addressing them are structured differently.
For the communicable and noncommunicable disease threats described above, public health activities are often focused on the individual; vaccinations and screenings are examples. In contrast, activities addressing risk behaviors often involve edu-

cational intervention targeting broader populations or population subgroups. These activities include programs related to preventing or facilitating the cessation of tobacco use and other types of substance abuse, improving physical activity and nutrition, and encouraging injury prevention through the use of seat belts or bicycle helmets.

4. Environmental exposures. As with risk behaviors, environmental exposures are not fully separate from communicable or noncommunicable diseases; these exposures are threats because they can cause communicable or noncommunicable diseases. For example, environmental exposures include food- and water-borne infectious agents.[7] Nevertheless, environmental exposures are generally considered a separate focus for public health, and often involve public health professionals who specialize in these areas. Further, public health activities addressing environmental exposures generally occur broadly, involving programs that could affect the health or larger population groups rather than focusing on the individual. Public health activities related to environmental exposures include inspection of foods and food processing/preparation facilities and water and air quality testing. Activities in this category of threat also include interventions related to potentially hazardous exposures in the "built environment," such as activities to monitor and minimize exposures to dangerous substances (e.g., asbestos) or other threats (e.g., radiation, excessive noise) in the workplace, homes, or public structures.

We intentionally developed this framework, based on the threats that are the focus of many public health activities and the desire for a parallel structure that can be applied to cyber security, to include the two broad categories of diseases (communicable vs. noncommunicable) and two additional categories of public health threats (risk behaviors and environmental exposures). There is clearly overlap between the two disease categories and the two additional threat categories. For example, participation in health risk behaviors can increase the risk for communicable diseases (e.g., blood-borne infections transmitted via intravenous drug use) and noncommunicable diseases (e.g., smoking and lung disease). Similarly, environmental exposures can include infectious agents (e.g., Salmonella bacteria) as well as pollutants (e.g., mercury or asbestos) that increase the risk of noncommunicable diseases. However, in categorizing different types of public health threats to use as a framework for considering cyber security threats, we felt that including risk behaviors and environmental exposures as separate threat categories was crucial for two reasons:

1. The types of public health responses to risk behaviors and environmental exposures is often different than the responses to communicable or noncommunicable diseases that do not occur as a result of risk behaviors or environmental exposures.

2. There are additional types of health impacts, such as head injuries, burns, and hearing loss, that can result from risk behaviors or environmental exposures and are the focus of public health activities, but are not disease conditions (although they may predispose effected individuals to subsequent diseases).

Although the goal of public health is to protect or improve the health of groups or populations, public health interventions can be broadly classified into two categories based on the unit or level being targeted by an intervention: interventions implemented at the individual level versus those performed at the system (organization, population group, or society) level. Examples of individual-level public health interventions include vaccinations, screening for infectious diseases (e.g., HIV, tuberculosis), cholesterol screening, and smoking cessation counseling. All of these interventions necessitate direct interactions between a health care professional and a potentially at-risk individual.

In contrast, system-level interventions rarely involve professionals whose main activities focus on the delivery of medical care. These interventions seek to reduce the risk of public health threats to large groups of people through a planned action or program rather than focusing on interactions with each individual separately. System-level public health interventions include educational campaigns, implementation of government laws or programs, and policies to reduce or prevent contact with potentially harmful exposures.

In addition, individual-level interventions can be broadly classified into three groups:

- Primary prevention: addressing a potential threat before it can affect an individual
- Secondary prevention: responding to a threat after an individual has been affected but before an adverse impact of the threat has developed
- Tertiary prevention: intervening after an adverse impact of a threat has developed to prevent worsening of the impact

Lessons Learned From Programs and Interventions Addressing Public Health Threats

Based on the framework described above and a review of public health literature, there are a number of important lessons from previously-enacted public health programs and interventions that have relevance for cyber security:

1. For public health interventions to be successful, recipients need to first recognize that a threat exists for which public health interventions would be beneficial. For this to occur, communication is vital. Easily understood information needs to be provided to a diverse audience using a variety of media or communications channels. Overall the goal is to engage and activate the target population. That is, to show that the public health threats are relevant to the target population—that these problems could affect them—and that there are actions they can undertake to address these threats.

2. Once the nature and potential severity of a public health threat is understood, individuals who may receive public health interventions need to be assured of the safety and effectiveness of the proposed interventions from a credible source. The goal here is to introduce potential solutions in a way that establishes a measure of trust.

3. Public health interventions need to be provided in a convenient and attractive (or at least not unattractive) framework. Even if there is belief in the importance of a public health program (e.g., decreasing obesity), individuals will not support or engage in it if participation is difficult, expensive, or incon-

Table 1.
Comparing Public Health Threats With Cyber Security Threats

Public Health Threat Categories	**Definition**	**Cyber Security Threat Categories**	**Definition**
Communicable public health diseases	Threats that are directly spread between individuals or can be transmitted between individuals by a nonhuman vector (e.g., tuberculosis, malaria spread by mosquitoes)	Cyber Security Communicable Threats	Threats that are directly spread between host computers or network hardware/software or, more commonly, are transmitted through ISPs and other backbone Internet providers prior to host- or network-level infection
Noncommunicable public health diseases	In contrast to communicable diseases, these threats that are not spread among people, but people may be at higher risk as a result of communicable disease exposure (e.g., HPV increases cervical cancer risk). Threats often worsen/evolve over long periods of time, and may go from being asymptomatic (detectable only by special screening tests) to having severe effects on quality of life and mortality	Cyber Security Noncommunicable Threats	Some threats are not spread among host computers, but similar to public health, the risk of these threats can be increased as a result of communicable cyber threats (e.g., a cyber virus can be used to launch attacks on others). These threats may affect your computer's performance as well as impacting others security..
Public health risk behaviors	Threats that are based directly on individual actions that may result in communicable or noncommunicable diseases (e.g., intravenous drug use, smoking) or may result in nondisease conditions (e.g., trauma from not wearing a seatbelt in a car)	Cyber Security Risk Behaviors	Very similar to public health, many cyber threats are based directly on individual actions which result in communicable and chronic threats (e.g., going to risky websites, not installing antivirus software, giving out passwords by phone)
Public health environmental exposures	Similar to risk behaviors, these threats may result in communicable diseases, noncommunicable diseases, or injuries, but these threats are based on exposure to pathogens, chemicals, or other hazardous materials (e.g., radiation) at potentially harmful levels in food, water, air, or the surrounding environment (which can be either natural or man-made)	Cyber Security Environmental Threats*	Threats that interfere externally (i.e., external to a computer or a network) with transmission of information can be considered environmental threats. This could include cut computer transmission lines (as occurred a few years ago with some trans-Atlantic lines), problems with satellites, or issues that interfere with wireless networks
N/A	N/A	Coordinated Cyber Security Threats	Threats that require manual, coordinated, or time-specific action as opposed to more automated (i.e., developed, distributed, and then largely ignored)

*Cyber security environmental threats will not be a focus of this paper as the subject of individual cyber risk preferences is not relevant to this type of threat.

Table 2. Characterizing Cyber Security Threats Using a Public Health Scheme

Type of Cyber Security Threat	Definition	Communicable	Noncommunicable	Based on Risky Behavior	Coordinated
Trojan horse programs	Threats hidden in a seemingly legitimate program	X		X	
Back door and remote admin programs	Programs with unknown access "holes"	X	X		X
Denial of service attack	Attacks in which many computers all attempt to access a website or network resources				X
Being an intermediary for another attack	Host or network being used as attack vector/origin	X	X		X
Unprotected Windows shares	Microsoft Windows share folders/drives are created but not adequately secured		X	X	X
Mobile code	Code written for mobile websites that may allow access to information on mobile phones		X	X	X
Cross-site scripting	A malicious script that is transferred to a computer through a URL link, database query, etc		X	X	X
E-mail spoofing	E-mails purporting to be from a trusted source asking for sensitive information or driving traffic to a bad website	X		X	X
E-mail-borne viruses	E-mails with malicious programs attached or links to malicious programs			X	
Hidden file extensions	A file name that appears to be a certain file type but is not.		X		
Chat clients	Chat programs such as AOL IM, Skype, or ICQ being used to send malicious programs attached or links to malicious programs		X	X	
Packet sniffing	A program that captures data from information packets as they travel over the network.				X

venient. To participate, individuals must believe that they will be able to successfully achieve the intended health objective.

4. Information on the nature of public health threats and available interventions needs to be communicated to a wide variety of audiences. Special attention is needed for audiences who are parts of disparate or particularly vulnerable populations, as they may be at increased risk for certain threats but less likely to receive or respond to information on these threats.

5. Multiple organizations (governmental and nongovernmental) need to be involved in responding to a public health threat. There needs to be adequate coordination among these organizations, including rapid communication and sharing of information as well as delineation of roles and responsibilities. Without this coordination, there are substantial barriers to both tracking and responding to potential threats.

6. The unpredictability of individual behavior must be considered. That is, individuals will often engage in activities that may not appear to have a rationale or scientific basis to public health policy makers. Plans need to be made to address reluctance to participate in public health interventions, ranging from increasing communications as to the benefits of a public health program, providing benefits for participating, or instituting negative consequences for not participating.

Section 4: How Does Cyber Security Fit In?

In contrast to the complex, multiparty public health systems and taxonomies described above, the cyber security community is very individualistic and much less rigorous in its analysis of successes and failures. Most of the efforts of the cyber security community are put toward finding new solutions and little attention is given to ensuring adoption or efficacy of these solutions. In fairness, there are not well-accepted metrics for "success" in cyber security—success generally implies a reduction in threats, vulnerabilities, or losses, but each of these is difficult to quantify, and thus widespread disagreement exists over how to determine whether an intervention works. Further, there are significant barriers to collecting information on the effectiveness of cyber security practices (e.g., legal issues regarding the collection, storage, and distribution of personally identifiable information). As such, there is no equivalent in cyber security to public health laws requiring reporting of communicable disease outbreaks or environmental exposures, and no parallel to state and national registries tracking trends in cancer and other noncommunicable diseases.

Given that the cyber security community lacks a suitable framework for both identifying and evaluating solutions, attention has turned to public health as a potential model for cyber security. Many cyber security threats and intervention strategies are well suited to be reviewed through a "public health lens." However, putting all cyber security threats and interventions into the same framework is no easy task. As described above, in public health, threats can be grouped by several primary categories, which are often overlapping. Cyber security threats can be thought of as having similar attributes that can help to differentiate or classify them. Table 1 aims to connect the high-level categories of public health threats with categories of cyber security threats.

As shown in Table 1, the standard public health characteristics all have relevance to cyber security, except for "environmental exposure" which is largely not relevant in describing common cyber security threats.[8] Cyber security threats are attributable to an "attacker," which is not the case in public health. As such, a new threat category was added in Table 1 for cyber threats to help describe the coordinated nature of some cyber threats. However, coordinated responses are part of public health interventions addressing all four types of public health threats presented in the framework discussed above.

Table 2 provides an overview of how various specific types of cyber security threats can be classified or defined using the four cyber security threat categories introduced in Table 1.[9]

Cyber security solutions can also be described and categorized using a public health frame of reference. Table 3 provides a taxonomy of cyber security intervention strategies for individuals based on the public health framework presented above.

Primary prevention strategies in cyber security include avoiding risk behavior (e.g., Internet users visiting untrusted websites or giving out their passwords by phone or e-mail to someone whose identity they do not sufficiently verify)[10] and maintaining good "cyber hygiene," including installing and updating a firewall and antivirus software. Each of these activities can help to prevent an Internet user from unintentionally allowing a virus, worm, or other type of malicious software to be installed on their computer in the first place. Prevention strategies such as these are not 100% effective at preventing malicious software or malware from being installed on a computer, but they do prevent the vast majority of threats.

Secondary prevention techniques would be used to both identify problems that are present (the equivalent of "screening" in public health) and to remove problems once they have been identified. For example, a computer is running slowly and may have various malware running on it. First, the computer would be scanned using antimalware software to look for threats. Thereafter, similar software would be used to remove these threats, if possible without causing damage to legitimate files. If caught early, largely such threats can be mitigating without catastrophic damage to the system.

Finally, tertiary prevention techniques would be used once the threat has already been causing damage, such as mining data on a host computer (e.g., for credit card or other personal information), attacking other computers or systems, or damaging files on the host computer. Interventions like this have a lower rate of success because the threat has already done some damage and long-lasting harm may be unpreventable. However, deep analysis, often more manual versus automated antimalware tools, can often help to salvage some or all of legitimate files and system components and to prevent damage from similar attacks in the future.

Table 4 provides a taxonomy of cyber security system-level interventions for the four classes of cyber security threats. The solutions described are actions which could be taken by a government agency—likely only the federal government would have the technical capabilities—or by certain private party actors such as Internet Service Providers (ISPs) and, in some cases, organizations such as nonprofit information-sharing consortia, which interact with large numbers of computer users

Table 3: Individual-level Interventions for Cyber Security Threats

		Cyber Security Threat		
		Viruses and worms (e.g., computer viruses and worms installed on a computer)	Poor behavior (e.g., freely open e-mail attachments and trust all websites)	Distributed attacks (e.g., DDoS attack aimed a shutting down server)
Type of Intervention				
Primary prevention—avoid threat	Avoid "high-risk" behavior	X	X	
	Firewall	X		
	Antivirus software	X		
	Other primary prevention	X	X	
Secondary prevention—address threat soon after onset to minimize damage	One-time or short-term interventions	X		X
	Ongoing interventions	X	X	X
Tertiary prevention—intervene to prevent fully present threat from worsening		X	X	X

Table 4: System-level Interventions for Cyber Security Threats

	Cyber Security Threat			
	Communicable	Noncommunicable	Risky Behaviors	Coordinated
Type of Intervention (at the System Level)				
Quarantine of affected Individuals (by ISPs)	X			
Mandatory individual-level interventions (e.g., Network Access Control)	X		X	
Monitoring of potential threat sources (by ISPs, government, or nonprofit group)	X			X
Secure configuration management				
Regulation of security of software*	X	X	X	X
High priority patching*	X			X
Mandatory reporting of new cases for assessment of breaches/trends*	X	X		X
Educational information describing risk factors	X	X	X	X
Guidelines/recommendations for early detection	X	X	X	
Potential civil/criminal penalties			X	X

* These interventions are not widely used and are largely industry specific or specific to a certain type of data breach/release.

and act as sub-systems. Similar to public health, some system-level interventions target individuals, but focus on broader activities that are likely to benefit larger groups. . Of note, however, many of these actions have not been to date taken or have only occurred in small settings, such as within a business or in a pilot program.

Quarantining of individual computers or computer systems that have been affected or are suspected of having been affected by a certain type of cyber security threat is a way to protect others from being affected by the same threat.[11] For example, quarantining may be appropriate for home Internet users suspected of having been turned into "bots" (i.e., part of a large network, called a botnet, that is being used to attack other individuals or organizations for a variety of malicious purposes). Alternately, a system (in this case an ISP) may reduce home Internet users' Internet speed or only allow them to use certain ports to connect to the Internet, thus restricting the applications they can access and the harm their insecurity may be able to cause to others. More commonly, many companies restrict their employees' access to certain websites to reduce the threat to their computer and reduce the threat to company data that may be purposefully or unintentionally manipulated by an insider. From a public health perspective, this may be thought of as a reverse quarantine (restricting where you can go rather than preventing you from leaving a fixed location) or perhaps the equivalent of travel restrictions (i.e., recommendations not to travel to certain areas due to the increased risk of communicable diseases in those areas).

As in public health, most system-level cyber security interventions focus on activities that are likely to benefit large groups. For example, organizations such as U.S. CERT in the United States currently seek to collect, aggregate, and disseminate such information. Private companies who sell threat information, such as McAfee and Symantec, also identify "threat signatures" that are used by their software packages to help stop threats. As a result of several regulations, many companies are required to implement "solutions" that identify and seek to mitigate threats (e.g., to personal financial information or personal health information held by private companies). If a significant data breach is discovered (e.g., when more than 500 health records are breached), companies are often required to disclose such to the U.S. federal government and contact affected individuals. A new SEC law may result in additional requirements that certain businesses report breaches that occur more broadly than those that affect certain data types.

Another group of system-level interventions includes environmental strategies aimed at mitigating or preventing threats. For example, a multitude of state and federal laws regulate certain types of security controls and tools that must be used to protect data from unauthorized access, and the procedures that must be followed when certain types of data are breached. Further, educational materials on risky behaviors (e.g., for home Internet users) as well as recommended guidelines for early detection of cyber threats (e.g., by businesses) are available targeting many types of threats. Such information is available through government agencies, nonprofit organizations, industry associations, and professional societies, among other organizations.

When attribution of an attack is possible, criminal or civil consequences may be associated with high-risk behavior and environmental threats. Different from public health, in cyber security the threat almost always originates from an individual or group. As such, when the economic impacts are sufficient to warrant investigating and when the attacker can be identified, criminal penalties and possibly civil consequences can result.

In seeking to use a public health framework to better understand and analyze cyber security, one important area of focus is disparities. In public health terminology, disparities exist when individuals belonging to minority groups, lower socioeconomic status populations, or other underserved individuals are more likely to experience the consequences of communicable diseases or environmental exposures, more likely to engage in certain risk behaviors, less likely to have early detection of and appropriate care for non-communicable diseases, and more likely to have impaired quality of life and decreased life expectancy because of public health threats. This is often considered to be a failure of public health.

It is likely that from a cyber security perspective, certain population groups are similarly more likely to experience adverse cyber events or less likely to have "protections" against these adverse events. Although likely smaller in magnitude, this cyber security divide (if it exists) may be related to economics (i.e., sufficient money to purchase appropriate protections), education (knowledge of the existence of an appropriate use of protection), and risk behaviors (willingness to engage in unsafe cyber practices).

Section 5: Conclusions and Recommendations for Research and Policy

The public health community has been very successful in identifying, monitoring, and reducing the health impacts of many types of threats. Given the many similarities between public health and cyber security, the cyber security community would be wise to leverage relevant public health strategies and analysis techniques. Certainly not all public health strategies will have a comparable approach in the cyber security community. For example, many public health threats are the result of naturally-occurring pathogens or biological events; in contrast, in cyber security, the vast majority of threats are man-made.

Although developing a robust community of cyber security stakeholders organized in any way similar to the complexity and scale of public health is daunting, the use of public health research strategies to better understand cyber security risk preferences is a specific area that should be leveraged in the short term. In the future, we plan to use public health risk perceptions research aimed at understanding preferred characteristics of vaccines to stop specific public health threats (e.g., measles) as a model to assess preferences associated with computer antimalware software to more effectively stop certain cyber security threats (e.g., computer viruses). Such research will constitute a first step at leveraging the public health community's analysis of risk preferences to improve cyber security.

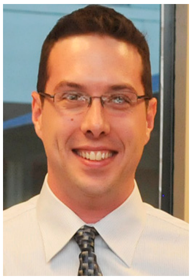
ABOUT THE AUTHORS

Brent Rowe is a senior economist at RTI and director of RTI's San Francisco office. His research focuses on technology policy and security issues. Past work has included assessing the market for Internet service providers to provide more security to home Internet users, estimating home internet users' cyber security risk preferences using a public health framework, conducting a cost-benefit analysis of the National Strategy for Trusted Identities in Cyberspace, and developing economic data to support cyber security strategic planning for NIST. Mr. Rowe is a member of IEEE and has served on numerous government panels and conference committees on cyber security and technology economics. In 2007, he co-authored Cyber Security: Economic Strategies and Public Policy Alternatives.

RTI International
114 Sansome St., Suite 500
San Francisco, CA 94104
Phone: 415-848-1317
Fax: 415-848-1330
E-mail: browe@rti.org

Michael T. Halpern, MD, PhD, MPH, is a Senior Fellow in RTI's Division of Health Services & Social Policy Research. His work focuses on health services, epidemiological, and outcomes research, including evaluations of public health programs; medical technology assessments; health care policy development; and analyses of medical care treatment patterns and quality of care. He is a member of the American College of Preventive Medicine and the American Society of Clinical Oncology.

RTI International
701 13th Street NW, Suite 750
Washington, DC 20005
Phone: 202-974-7813
Fax: 202-974-7855
E-mail: mhalpern@rti.org



Tony Lentz is an economist in the Environmental, Technology, and Energy Economics program at RTI International. Mr. Lentz specializes in the application of economic models to analyze agricultural, environmental, energy, and natural resource regulations, programs, and policies. He has experience conducting projects for the U.S. Environmental Protection Agency, the U.S. Department of Agriculture, DHS, and other government agencies to analyze the economic impacts of climate change, greenhouse gas emissions, renewable energy, energy efficiency, technological innovation, and regulatory compliance.

RTI International
3040 Cornwallis Road
Research Triangle Park, NC 27709
Phone: 919-541-7053
Fax: 919-541-7155
E-mail: alentz@rti.org

REFERENCES

1. Mulligan, D. K., & Schneider, F. B. (2011). "Doctrine for Cybersecurity". Daedalus, 140(4), 70–92.
2. Charney, Scott. Collective Defense . Applying Public Health Models to the Internet. Microsoft, 2010.
3. Department of Homeland Security (DHS). (2011). "Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action". Available at: <http://www.dhs.gov/xlibrary/assets/nppd-healthy-cyber-ecosystem.pdf>.
4. Centers for Disease Control. Ten Great Public Health Achievements --- United States, 2001–2010. Morbidity and Mortality Weekly Report, May 20, 2011; 60(19);619-623.
4. Charney, Scott. Collective Defense . Applying Public Health Models to the Internet. Microsoft, 2010.
5. Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). "Studying Users' Computer Security Behavior: A Health Belief Perspective". Decision Support Systems, 46(4), 815–825.
6. IBM. Meeting the cybersecurity challenge: empowering stakeholders and ensuring coordination. <https://www-304.ibm.com/easyaccess3/fileserve?contentid=192188; Feb. 2010>.
7. Institute of Medicine. 2008. The Future of Public Health. National Academy Press, Washington DC, page 1.

NOTES

1. <http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf>
2. For example, see Bruce Schneier's 2008 essay on the subject at <http://www.schneier.com/essay-155.htm>.
3. <http://www.whatispublichealth.org/>
4. <http://sph.washington.edu/about/whatis.asp>
5. Our proposed framework is clearly not the only framework that can be used to classify public health threats. However, we believe this framework does capture the main categories of threats in a comprehensive and efficient manner that lends itself to examining parallels with cyber security threats.
6. It is also important to consider that almost any behavior (e.g., eating a meal, crossing a street) can lead to adverse health consequences. In the context of this paper, we consider risk behaviors to represent conscious actions that increase the likelihood of adverse health consequences beyond that experienced as part of standard activities of everyday living (however that is defined).
7. In the context of this paper, we consider environmental exposures to be those exposures that increase the risk of adverse health consequences beyond the baseline experienced during standard (or even optimal) periods. Further, environmental factors are generally considered passive; that is, an individual is often subject to an environmental exposure without his or her knowledge or choice, while participation in a risk behavior implies a conscious choice.
8. Note that there is a type of cyber threat that could be considering as "natural" or similar to an environmental threat to public health. Anything that interferes externally (i.e., external to a computer or a network) with transmission of information would fall into this category. This could include cut computer transmission lines (as occurred a few years ago with some trans-Atlantic lines), problems with satellites, or issues that interfere with wireless networks. Although there is this category of "environmental cyber threats," for our purposes, they are outside the scope of this discussion which focuses on issues more directly related to cyber threats.
9. This list comes from CERT at Carnegie Mellon. See <http://www.cert.org/tech_tips/home_networks.html>.
10. Social engineering and phishing are common approaches used by cyber attackers to gain information such as passwords. In phone calls or e-mails, the attackers pretend to be a trusted source–a company IT helpdesk or bank employee–and ask for information which can be used to access their computer, e-mail accounts, bank accounts, etc. Such approaches are very common and often very successful.
11. <http://www.microsoft.com/en-us/news/exec/charney/2010/03-02rsa2010.aspx>