THE INTERNET HEALTH MODEL FOR CYBERSECURITY

EastWest Institute
Forging Collective Action for a Safer and Better World

ISBN: 978-0-9856824-2-2
Cover image by Dragan Stojanovski

The EastWest Institute is an international, non-partisan, not-for-profit policy organization focused solely on confronting critical challenges that endanger peace. EWI was established in 1980 as a catalyst to build trust, develop leadership, and promote collaboration for positive change. The institute has offices in New York, Brussels, and Moscow. For more information about the EastWest Institute or this paper, please contact:

The EastWest Institute
11 East 26th Street, 20th Floor
New York, NY 10010 U.S.A.
1-212-824-4100
communications@ewi.info

www.ewi.info

The Internet Health Model for Cybersecurity

Principal Author

Kevin Sullivan, Microsoft Corporation

Contributors

Sanjay Bahl, Consultant from India
Chris Boyer, AT&T
Erin Nealy Cox, Stroz Friedberg
Grant Fjermedal, Creative Logic Inc.
Igor Nai Fovino, Global Cybersecurity Center
Chauncey Holden, Fidelity Investments
Mark Hughes, British Telecommunications
Yurie Ito, Asia Pacific Computer Emergency Response Team (APCERT)
Luis Kun, CHDS at U.S. National Defense University
Alyssa M. Le Sage, CERT at Carnegie Mellon University
Americo Lenza, Vodafone
Joe Mitola, Stevens Institute of Technology
Michael O'Reirdan, Message Anti-Abuse Working Group (MAAWG)
Greg Rattray, Delta Risk
Karl Frederick Rauscher, EastWest Institute
Greg Shannon, CERT at Carnegie Mellon University
Joanna Sharpe, Microsoft Corporation
Joe St Sauver, University of Oregon and Internet2 Andy Steingruebl, PayPal
Michel van Eeten, Delft University of Technology
Maxim Weinstein, StopBadware
Li Yan, China Institutes of Contemporary International Relations (CICIR)
Jason Zabek, Cox Communications

FOREWORD

The foundations of our modern society are becoming ever more digital. More than two billion people are now on the Internet, with current projections estimating that number to grow by another billion by 2016. Cyberspace now provides a range of critical services to more citizens around the world than ever before. Governments depend on digital infrastructure to conduct business, enable services, protect public health and safety, and advance national defense and economic security—all essential to managing a modern nation.

Research shows that over the next few years the world will see an unprecedented growth in Internet users, devices, and data, which will continue to create vast opportunities for communication, collaboration, and commerce. As more people, computers, and devices come online, cyber criminals continue to grow more sophisticated in their abilities to gather sensitive data, disrupt critical operations, and commit fraud. Many countries have sought to improve public-private critical information infrastructure policy, to build effective information sharing and collaboration capabilities that address threats and vulnerabilities, and to coordinate on responses to increasingly complex cyber incidents. While use of and reliance on the Internet continues to grow, it is clear that governments, industries, and individuals will need to find innovative models and means for cooperation to reduce cyber threats that impact citizens. An Internet health model is a conceptual framework to help guide a global, coordinated approach to improving security on the Internet. Improving the health of the Internet requires a global, collaborative approach to protecting people from potential dangers online.

At the EastWest Institute's Second Worldwide Cybersecurity Summit in 2011, we led a workshop of global industry and government leaders with the objective of finding tangible and measurable ways to improve global Internet health. This paper, which stems from work following that session, concludes that there is no global, coordinated approach to protecting people and systems from malware and related threats on the Internet. Looking to the model of public health for inspiration, the group offers seven key principles to translate the concepts of public health into approaches for managing the cybersecurity of large populations. The contributors also provide an exploration of five areas for future research.

Threats to our information-centric society continue to grow apace with the number of users and devices that connect to the Internet. In order to disrupt this trend, we must find relevant models and adopt a coordinated approach to protecting people and systems online. This paper represents a solid first step in establishing the Internet health model as an organizing framework and identifying priority areas for future research. We urge the global policy and technology communities to develop an Internet health model that both protects individuals and balances the security and privacy needs of citizens, governments, and organizations worldwide.

Scott Charney
Corporate Vice President
Trustworthy Computing
Microsoft Corporation

Bryan Littlefair
Chief Information Security Officer
Vodafone Group Services Limited

EXECUTIVE SUMMARY

For individuals, businesses, and governments, the Internet supports communications, collaboration, commerce, and a world of other services. As a shared global resource, the Internet provides critical infrastructure for much of the developed and developing world. This same ubiquity has made the Internet a popular channel for launching cyber attacks from a range of bad actors in cyberspace.

Today, there is no global, coordinated approach to protecting people and systems from malware and related threats on the Internet. We must begin to create a more secure and defensible foundation for cyberspace now in order to protect the two billion current users and the next billion users expected online by 2015. We believe the solution lies in a coordinated international effort among governments and industry players across the IT ecosystem to protect the shared environment of the Internet from bad actors.

The model of the public health field provides a good starting point for developing a coordinated global effort to better protect users online. For example, the health of individuals and communities in society is improved through the collective actions of individuals themselves and frontline healthcare providers with the support, coordination, and guidance of organizations such as the World Health Organization (WHO) and the United States Centers for Disease Control and Prevention (CDC). While we do not suggest that the public health model provides a complete blueprint for securing the Internet, we believe that it can serve as inspiration for how to better protect cyberspace.

A public health agency, whether operating on the local, state, national, or international level, is a robust model for potential application to cyberspace, with basic functions including education, monitoring, epidemiology, immunization, and incident response. This paper examines what an Internet health model might look like as an approach, leaving details to be determined based on the needs of society. Those details may differ according to roles, sectors, national policies, and international needs.

The public health model, applied in accordance with the Internet health principles in this paper, can be broadly applied to cybersecurity challenges. While individuals must take ultimate responsibility for their online safety, they cannot do so in isolation. Accordingly, service providers and vendors, recognizing the responsibility and opportunity to help consumers stay safe online, can offer innovative products and services to improve and maintain the health of their devices. The Internet health model can help significantly decrease the ability of malware, botnets, and other threats to propagate across the Internet, and thus it can help protect society from cyber threats.

CONTENTS

Introduction

Cyberspace, the vast realm of the Internet and World Wide Web, stands as a monument to human ingenuity and innovation, delivering a range of communication services to people around the world. The Internet supports communication, collaboration, commerce, and a world of other services for individuals, businesses, and governments worldwide. As a shared resource, it provides critical infrastructure for much of the developed and developing world.

The International Telecommunication Union (ITU) reports that the number of Internet users reached two billion in March 2011, and Boston Consulting Group estimates that another billion users will come online by 2016.[1] Governments and organizations must work across borders to help ensure that this critical global resource is made more secure and resilient for citizens who are online—now and in the future. Global cooperation among industry and governments is needed, because threats to cybersecurity come from around the world. We must begin to create a more secure and defensible foundation for cyberspace now in order to protect the current two billion users and be more prepared for the next billion.

The same ubiquity that makes the Internet mission-critical for many users across the globe, also makes it a popular channel for launching cyber attacks for a range of bad actors. Malicious code (also known as malware or badware) is used by cyber criminals, organized crime rings, and state actors for financial gain, espionage, and breaking into private and government sector computer networks in search of intellectual property and classified documents. There is also concern that the Internet may someday be used to effect cyber terrorism or cyber warfare.

Protecting the global Internet has proven challenging, as the nature of the threat and structure of attacks changes with each defensive success. Today's operational cyber environments are complex and dynamic. User needs and environmental factors change frequently, leading to unanticipated use, reconfiguration, and continuous evolution of practices and technologies. New susceptibilities in these environments are continually being discovered, and the means to exploit these environments continue to proliferate.

While high-profile data breaches and targeted cyber attacks capture the headlines, much of the underground economy is driven by millions of infected home and business computers participating in botnets, stealing passwords, scaring users from using the Internet, and tricking people into buying fake products. Websites, advertising networks,

[1] https://www.bcgperspectives.com/content/articles/media_entertainment_strategic_planning_4_2_trillion_opportunity_internet_economy_g20/

Problem Statement:

There is no global, coordinated approach to protecting people and systems from malware and related threats on the Internet.

and search engines increasingly serve as inadvertent conduits for malware that spreads and infects unsuspecting users. Robotic networks, known as botnets, are pools of infected computers directed from a centralized command center that spread malware via people's computers and devices without user awareness. Botnets are now available for rent by malicious actors.

From the standpoint of national security, botnets are a threat to governments, because the same networks of hijacked computers that enable mass mailing of spam can also be used to attack critical infrastructure and disrupt communications.

In addition to the challenges of measuring compromised devices, the losses from cybercrime are also difficult to quantify, though total costs are large worldwide from the perspective of individuals, businesses, governments, and other Internet stakeholders. While direct monetary losses are easier to measure, perhaps the greatest losses come in the form of intellectual property losses by organizations and governments.

Government cybersecurity policy, once focused mainly on critical infrastructure and national defense, has shifted to include security threats to consumer devices. The consumerization of information technology (IT) and the "bring your own device" era in workplaces have blurred or erased many of the boundaries between enterprise and consumer environments, making it harder for IT administrators to secure systems and networks.

Networked environments will likely continue to be vigorously attacked for the foreseeable future. Public and private organizations will need to enhance their abilities to protect resources, detect attacks, and recover from successful exploits. While we anticipate such efforts will be accomplished locally within organizations, sectors, and countries, we must devise coordination structures and strategies to enhance global collaboration in the effort to protect cyberspace.

This paper is the result of an initiative that began with an interactive working session on Internet health at the EastWest Institute's Second Worldwide Cybersecurity Summit in London in June 2011. The multilateral group of experts and stakeholders originated with a half-day workshop at the summit and has continued monthly discussions focusing on the problem statement listed below. This paper serves to capture the salient points of those discussions and provide a reference point to begin future research and development necessary to build a global, coordinated approach to protecting people and systems from malware and related threats on the Internet.

Considering the Public Health Model

We believe public health can be a source of inspiration for measures to better protect cyberspace.

Turning to our problem statement—there is no global, coordinated approach to protecting people and systems from malware and related threats on the Internet—we believe the solution lies in a coordinated international effort, which would be the most efficient means for protecting the shared environment of the Internet from bad actors.

Inspiration

Considering what a coordinated international effort might look like, we believe the model of the public health field provides a good starting point. The health of individuals and communities is improved through the collective actions of individuals themselves and frontline healthcare providers, with the support, coordination, and guidance of organizations such as the World Health Organization (WHO) and the United States Centers for Disease Control and Prevention (CDC). We do not suggest that public health and related institutions provide a complete blueprint for securing the Internet, but we believe public health can be a source of inspiration for measures to better protect cyberspace.

The contributors to this paper chose to focus not on the details of specific efforts, but rather on how to develop a common model for addressing the issues, to encourage future efforts, and to accelerate the process of finding a solution. Members of our group represent a rich set of perspectives on this issue, and some framing ideas are represented here.

Our call for adoption of some form of a public health model is not novel. The concept has been included in literature for decades. The tendency to view malicious code as a biological entity goes back to the first definitions of computer viruses. A 2001 *Scientific American* article[2] traced the origins of the concept to a 1949 paper by John von Neumann ("Theory and Organization of Complicated Automata") and John Conway's "Game of Life" in the 1960s. The first publication the article found that used the term virus to describe self-replicating code was in the work of Frederick Cohen and Len Adleman in 1983.

Not surprisingly, once the computer industry began speaking of malicious code in terms of viruses, it wasn't a big leap to view solutions in terms of medicine. The idea of using a public health model as a framework to protect against the spread of viruses is found in an article by Jeffrey O. Kephart, David M. Chess, and Steve R. White in their 1993 paper "Computers and Epidemiology"[3] published in the *IEEE Spectrum*. More recently, Joe St. Sauver of the University of Oregon proposed a Cyber World Health Organization[4] and Scott Charney, Corporate Vice President of Trustworthy Computing at Microsoft, wrote a white paper[5] called "Collective Defense: Applying Public Health Models to the Internet."

2 https://www.scientificamerican.com/article.cfm?id=when-did-the-term-compute

3 http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=275061&tag=1

4 http://pages.uoregon.edu/joe/ecrime-summit/ecrime-summit.pdf

5 http://blogs.technet.com/b/microsoft_on_the_issues/archive/2011/02/15/advancing-the-idea-of-collective-action-to-improve-internet-security-and-privacy.aspx

A public health agency, whether operating on the local, state, national, or international level, appears to have robust application potential for cyberspace.

Functions of a Public Health System

The public health model has grown in relevance in recent years, and for good reason. A public health agency, whether operating on the local, state, national, or international level, appears to have robust application potential for cyberspace with a set of basic functions including:

- **Education.** A public health agency is charged with educating the public about proven safe practices: wash hands frequently, especially during epidemics; avoid contact with those who are infected with a contagious disease. And it raises public awareness of and offers solutions to health threats old and new. Once proven, a diagnosis, treatment, or practice is shared with everyone.

- **Monitoring.** A public health agency is often charged with monitoring its general domain (whether city, county, state, or national) and issuing alerts when it detects an upsurge in infections or other health problems. County agencies may report to a state body or plug directly into a national reporting system. This function provides an important early warning system to enable health agencies to respond more rapidly and with a more coordinated effort when problems arise.

- **Epidemiology.** Beyond monitoring, a public health agency, especially at the state or national level, employs scientists who serve as medical detectives. In the United States, this function is most clearly seen in the work of the CDC. Epidemiologists deeply study outbreaks to determine the cause and to provide guidance on remediation.

- **Immunization.** Actual immunizations are likely to be received locally, from physicians and nurses working in the community in either the public or private sector. However, a public health agency will often serve in a coordination and enforcement role. It can initiate voluntary immunization campaigns, helping the public to select countermeasures from the myriad and often confusing range of available options. Furthermore, it may require that children of a certain age have a specific set of vaccinations before registering for school.

- **Incident Response.** Public health agencies have incident response teams on a local and national level. Locally, health workers typically work with restaurants to contact customers, for example, in cases where a food services worker is found to have hepatitis; or in cases where a store or other provider sold food that may carry salmonella, E. coli, or some other form of bacterial infection. On the national level, an

While the public health field accepts the term surveillance as a tool for understanding the environment, it has a negative privacy connotation in cybersecurity.

agency, such as the CDC in the United States, will fly into a community whenever an unusually unexpected and threatening infection is found. The idea is to help those infected, while working to identify and isolate the source of infection before it can harm others.

The familiar public health scenario outlined above certainly lends itself toward addressing some of the basic elements that can logically form a beginning framework for protecting the Internet. The national Computer Emergency Readiness Teams (CERTs) and related organizations fill the role of national CDC equivalents, and international organizations act to facilitate rapid exchange of monitoring and epidemiological data and to help coordinate global responses.

Limitations to Consider

Our analysis of the public health approach also considered many of the concerns about applying this model to cybersecurity, including important differences:

- Diseases are organic, while malware originates from human intent.
- Most malware does not cause physical harm or death.
- Devices do not have natural immune systems.

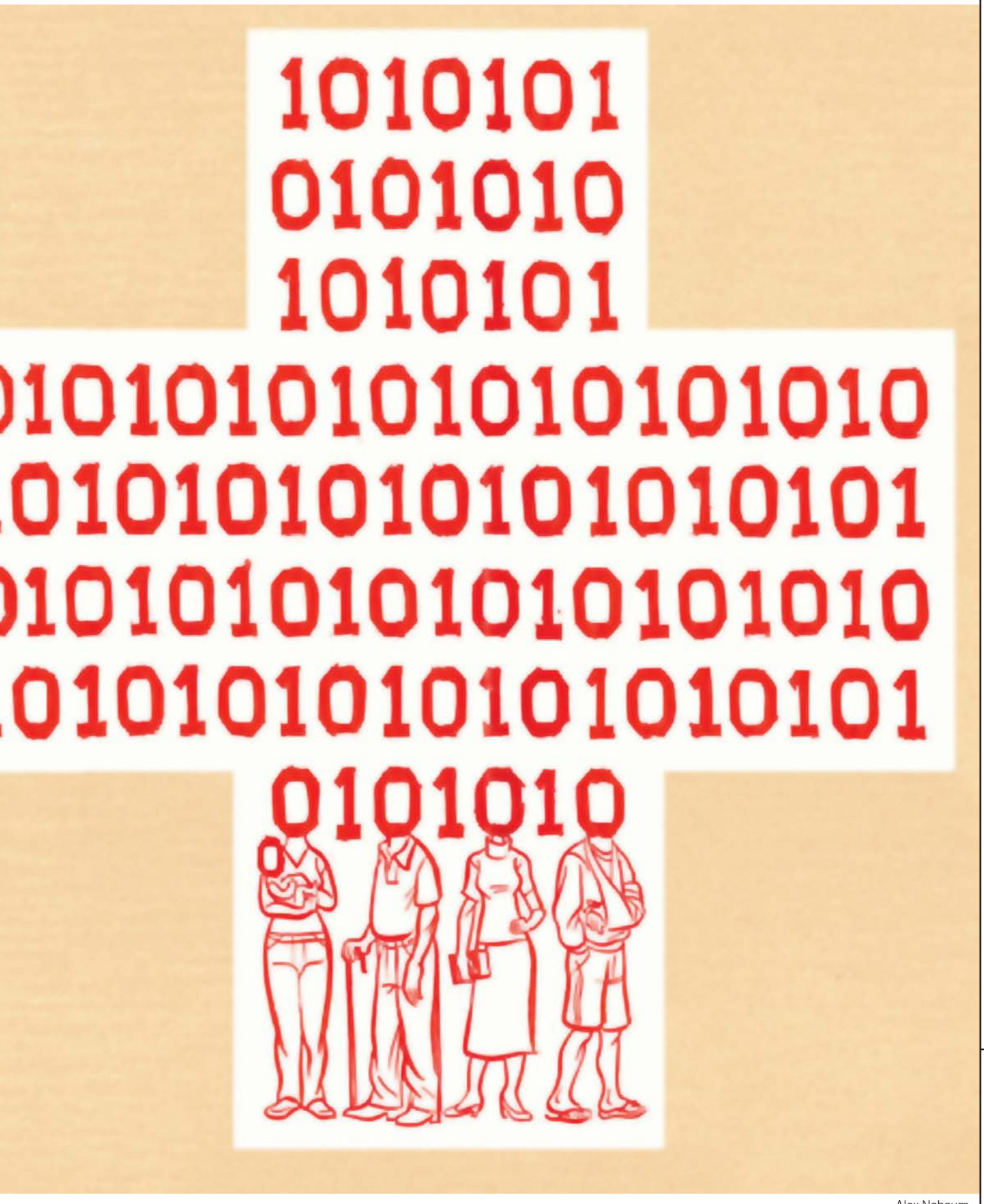
These concerns help highlight some of the limitations of the analogy, and they should be kept in mind as our proposed Internet health model evolves. Still, we believe the parallel with public health is instructive in building a framework for cybersecurity.

Additionally, the contributors identified two public health concepts that have some negative connotations in Internet security discussions:

- monitoring or surveillance
- quarantine

First, while the public health field accepts the term surveillance as a tool for understanding the environment, it has a negative privacy connotation in cybersecurity. Within the public health model, consider an example of syndromic surveillance where increased sales of orange juice and chicken soup may point to an influenza outbreak. Equivalent surveillance techniques on aggregate or anonymous data can be valuable in cybersecurity as well, but the community will need to find a way to address user privacy concerns. The second concept is quarantine—a public health tool used in limited situations around the world that also raises concerns in the context of Internet security. There are two types of quarantine that we must consider: separating the sick, and separating the healthy. As a community, we must weigh the benefit of protecting consumers against the risk of disrupting access to content and services.

Even though there are several areas where there is not yet consensus, the contributors established seven principles for an Internet health model to guide this work forward. The remainder of this paper is dedicated not to providing answers but to suggesting further what a parallel structure might look like. We hope this will encourage others to embrace the idea and to begin the process of filling in the details—details that may very well need to be quite different across roles, sectors, national policies, and international needs.


1010101
0101010
1010101
01010101010101010101010
10101010101010101010101
01010101010101010101010
10101010101010101010101
0101010

Alex Nabaum

An Internet Health Model for Cybersecurity

Internet health is a public good. The proper function of today's connected society, including global communication, collaboration, and commerce, requires a baseline of Internet health.

The Internet health model is a conceptual framework to help guide a global, coordinated approach to improving security on the Internet. In this paper, we look at the components of cybersecurity that protect consumers from the impact of malware and related threats. As in public health, we cannot judge success by complete eradication of problems, but rather by the magnitude and direction of trends.

To move from analysis of the public health model to applying the concept to cybersecurity, the contributors have developed the following principles:

1. Internet health is a public good. The proper function of today's connected society, including global communication, collaboration, and commerce, requires a baseline of Internet health.

2. Internet health depends upon shared responsibility. Internet users—both individual and institutional—must take responsibility for the health of their devices and networks. Users must also be supported by an ecosystem that enables and encourages healthy choices.

3. Internet health relies on evidence-based approaches. The success of the Internet health model depends on developing, documenting, and disseminating proven methods for diagnosis and treatment of security issues.

4. Internet health emphasizes prevention over treatment. The Internet health approach does not seek simply to improve the efficacy of treatment; rather, it aims to increase prevention of compromise and infection. While treatment is a natural function of public health, it is in the best interest of the ecosystem to help users avoid malware in the first place.

5. Internet health is a spectrum. While we may, in some cases, be able to identify a specific infection, the overall health of a device or network is not binary. There are multitudes of attributes that comprise the health of a system and should be considered in assessing its state.

6. Internet health efforts minimize potential harm. Efforts to prevent or treat "disease" should avoid impinging on the safe, legitimate use of devices and the Internet.

Public Health Function	Application to Cybersecurity
Education	Providing objective, evidence-based guidance for end users, organizations, and security practitioners about basic strategies for improving health, including prevention and remediation.
Monitoring	Monitoring digital networks for signs of compromise, intrusion, or other malicious behavior.
Epidemiology	Analysis of malicious code to understand how it was developed, the infection vectors, how it spreads, and the impact on end systems and users. Measuring infection rates and indicators of compromise, and providing general intelligence briefings.
Immunization	Based on the epidemiologic work, the IT industry, customers, and partners work to secure default configurations, close known exploitable coding errors, and rapidly distribute updates and protection tools.
Incident Response	CERTs and similar organizations coordinate response to massive infections and provide authoritative guidance to impacted parties.

7. Internet health efforts protect privacy. Protecting the privacy of users' behavior, data, and communications should be a primary consideration when collecting, inspecting, and sharing data about Internet health.

Using these principles to guide investigation and implementation, we believe the public health model can be successfully applied to cybersecurity in order to reduce the impact of botnets and malware on consumer Internet users. In the following section we will look at how the functions of public health can improve cybersecurity.

Reduce the Impact of Malware

The contributors believe that the concept of the Internet health model, including the principles above, can be broadly applied to cybersecurity. For this paper we focused on the steps that many private sector companies, non-profit organizations and governments around the world are taking to help protect consumers from the effects of malware. In many cases these efforts map closely to the functions of public health.

This paper submits that developing actions such as these will protect consumers from the impacts of malware on the Internet as well as many other issues not included in this paper. We believe these programs should continue to grow in a scalable and coordinated manner to provide effective protection against evolving threats to all Internet users. The following section explores what the contributors believe to be a priority list of topics for further investigation necessary to improve the effectiveness, scalability, and coordination of a public health approach to cybersecurity.

Themes for Further Development

For the Internet health model to be successful, necessary monitoring activities must be matched with appropriate controls.

We believe that the public health model provides a robust framework for creating a collective defense against cyber criminals and other bad actors in cyberspace. We see private entities, CERTS and public-private partnerships playing both individual and collaborative roles in a public health model for cybersecurity. While it is not the intent of this paper to prescribe a solution, we hope that exploring potential building blocks and interconnections of cybersecurity will give rise to discussion and research that will lead to efficient methodologies that promote global Internet health.

As we look toward the need for implementing some form of a public health model to enhance security across the Internet, we see at least five areas in which additional research and development may prove beneficial:

- addressing the consumer experience of the Internet health model;
- developing systematic and targeted education and awareness efforts;
- exploring the division of roles and responsibilities among ecosystem entities;
- establishing metrics, measurement, and information sharing schemes; and
- evaluating policies and technology for treating malware and promoting good hygiene.

User Experience

While we expect the Internet health model to apply to cybersecurity issues broadly, reducing the impact of malware on consumers is our primary focus in this paper. In order to provide the most benefit to consumers and reduce the likelihood of unintended consequences, we must thoroughly examine the user experience of the Internet health model. This ranges from their perceptions and expectations about security to building trust between parts of the ecosystem and balancing security and privacy.

Perceptions and Expectations

It is important to understand consumer perceptions and expectations with respect to security of their Internet connected devices and services. A full user study is beyond the scope of this initiative. We will, however, outline the following observations to consider in the development of the Internet health model.

- **User expectations and abilities** regarding Internet health responsibilities differ significantly among consumers, small businesses, governments, large corporations, and global multinational entities. Consumers and small businesses generally expect their cybersecurity to be provided by whatever device or service they use to go online. Gov-

ernments, large corporations, and global multinationals can be expected to demand more control and flexibility over how they secure their systems and manage risk, as they have their own internal IT resources to deploy firewalls, monitor systems behavior, train users, and take other measures.

- **Users own their devices and bring them into the enterprise.** As personal technology becomes more powerful and affordable, users are increasingly providing their own technology and bringing it into the workplace. This consumerization of IT has security implications for enterprises as consumer devices generally do not come with enterprise-level support, something that must be considered under the Internet health model.

- **Users' software choices are changing.** Increasingly consumers are adopting web- or cloud-based services for everything from email to document editing, replacing traditional desktop applications. The shift is expected to change the model and roles for those implementing the Internet health model.

Security Enhances Privacy

One of the Internet security community's objectives is to reduce the population of consumer computers that are susceptible to or already part of a botnet. To do so, it is necessary to identify with the best possible accuracy the infected and susceptible consumer, small business, government, and corporate computers and other devices (including industrial control systems) attached or capable of attaching to the Internet. We recognize that the idea of monitoring for infected devices makes some people uneasy, and gives them a feeling of compromised privacy. In most cases, however, monitoring for signs of infected devices is distinct from monitoring of content or identity. For example, when an ISP receives information about infected machines in its network, it can reach out to its own customer directly. Successful remediation does not require another party to know the identity of the customer. For the Internet health model to be successful, necessary monitoring activities must be matched with appropriate controls to ensure that abuse is deterred, suspected abuses are readily and openly investigated, and detected abuses are remedied openly and effectively.

Monitoring for infected devices may be an effective means to help enable privacy. Without the ability to detect and remove malware from user's devices, there is no privacy. Potentially every keystroke made by a user can be monitored by malware. Depending on the intent and functionality of the malware, an infected machine can provide a backdoor from which bad actors can extract files, intellectual property, passwords, financial data, and whatever else might be of interest to them. To counter this, we might consider how the systems and process of the Internet health model can serve as privacy enhancing technologies.

Building Trust

For the shared responsibility of Internet health to succeed, we must focus on building trust between related parties. These efforts can involve building trust in the relationship that exists between consumers and service providers; service providers and other service providers; service providers and vendors; and between governments. Consumers must be able to trust that their service providers are committed to their safety and security and not motivated nor solely interested in them for commercial purposes. Service providers must trust that vendors are providing effective solutions. Governments must have mutual trust in order to facilitate information sharing and law enforcement activities critical to increasing Internet health.

We also note, with caution, the potential collusion of price and trust. While there are many free or very low-cost tools and services to help prevent or remediate malware, there are circumstances that require paid products and services. There is no expectation that a service provider or vendor provide goods and services at no cost. However, we urge caution in how paid offers are promoted to consumers. The requirement to pay upfront, especially when accompanied by a scary warning, is a favorite tool of scammers. We need

Governments must have mutual trust in order to facilitate information sharing and law enforcement activities critical to increasing Internet health.

providers of free and paid services alike to be able to distinguish their offerings from fakes, thus further building trust with consumers.

Developing Systematic and Targeted Education and Awareness Efforts

Consumer security programs traditionally focus on public education and awareness to give users methods and resources to better protect their computers and networks both before and after they experience a security incident. We observe that in the realm of human health, most individuals do not need to experience a traumatic injury or serious disease to learn about basic health risks. Increasing consumer understanding of online risks can achieved with both broad awareness efforts aimed at prevention and targeted teachable moments in the wake of an incident. Doing so requires educational messages to be:

- prioritized based on evidence of effectiveness;
- consistent across providers and domains; and
- integrated into other elements of Internet health, including detection, notification, and remediation.

Prioritized Based on Evidence of Effectiveness

The third of our seven principles for Internet health calls for evidence-based approaches to detecting and remediating cybersecurity issues, specifically botnets and malware. The general Internet user is not a security expert and has many competing demands for time and attention. We cannot expect them to experimentally treat a malware infection on their device. Instead, as a community, we must develop, document, and disseminate the proven methods for detection and remediation.

Consistent Across Providers and Domains

We recommend the development of consistent guidance across providers and domains

Mike Lemanski

in providing security information and processes to consumers. Increasingly, consumers procure online services from a variety of providers. Some of these are even in the same domain, for example with a consumer that uses more than one online bank. As more of these providers adopt the shared responsibility for Internet health, it is essential that they not provide conflicting guidance to consumers. Note that this does not eliminate the possibility of differentiation of security services or prevent service providers from having flexibility in how they interact with their customers. Rather it calls for some baseline consistency in the core messages and processes that service providers communicate to consumers. As changing consumer behavior is a long-term effort, these consistent core messages should also be reflected in broad outreach educational curriculum.

Integrated with Detection, Notification, and Remediation

Finally, education and awareness efforts should be integrated with detection, notification, and remediation. The goals of the Internet health community should include continually educating users so that they become aware of the potentially disastrous consequences of the highest priority security threats. This knowledge enables users to protect themselves against threats, for instance by taking care to avoid the ever more sophisticated social engineering techniques that are often a precursor to the propagation of dangerous malware.

Education also should include training consumers and other less sophisticated users on how to avoid fraudulent security products (e.g. antimalware, identity protection, etc.) that are commonly promoted today. Those parties involved in education and notification efforts should take care to ensure that their users are able to confidently distinguish the genuine tools provided from malicious fakes. Similarly, users will need to learn the importance of recognizing these genuine tools and how to access them rather than responding to fraudulent anti-virus messages that simply pop up on the screen.

It's not necessarily clear where Internet health responsibilities are held and shared between entities including governments, CERTs, ISPs, online service providers, software vendors, and other players.

Exploring the Division of Roles and Responsibilities Among Ecosystem Entities

In public health there is a relatively clear hierarchy of providers and information aggregators—from the WHO to the CDC, state and regional public health agencies and hospitals, to the physicians, pharmacists, technologists and other service providers. Cybersecurity does not have the same clear hierarchy or structure. It's not necessarily clear where Internet health responsibilities are held and shared between entities including governments, CERTs, ISPs, online service providers, software vendors, and other players. This makes the question of division of responsibility a rich area for discussion and exploration.

Figure one illustrates an oversimplified malware-related scenario and shows the variety of roles at play. To begin, a cybercriminal gains unauthorized access to a website hosted in another country and loads malicious code on the site. Second, a consumer in yet another country browses to this same website, which results in infecting their device. Now that their device is infected, the malware can watch for the consumer to conduct online banking transactions and then steal their username and password. Finally, armed with these credentials the criminal can illegally transfer money out of the victim's account.

This simple example involved up to four different countries and at least as many entities in the response. Law enforcement should deal with the criminal, while a web hosting company helps remove the compromised site. At the same time the bank is conducting an investigation and the consumer's ISP may notify the user of their compromised device. There may additionally be several other national or international organizations involved in detecting the compromise, notifying the victims, and helping to mitigate the threat.

It is clear that many organizations need to be involved in the successful prevention or remediation of malware threats. In order to effectively coordinate these responsibilities, entities should focus on the capabilities they are best suited to provide support to existing customer or partner relationships. In the example above, web-hosting companies are best suited to detect and remove compromised websites while ISPs can detect compromised consumer devices and provide notice to the affected customer. Banks and other online services may also provide notifications about current online threats to impacted customers. Additionally, national or industry CERT teams can help facilitate data exchange and resolve cross-border policy issues. The contributors have examined the five stakeholder groups below as a starting point for the shared responsibility of an Internet health model.

Government

While there seems to be little disagreement that governments will play a critical role in carrying and sharing responsibility for enhancing cybersecurity, opinions vary as to exactly what responsibilities they should carry and how they might best exercise those responsibilities.

Some of the areas in which government might play a role include:

- **Removal of barriers.** Governments are well suited for mediating between interest groups and helping to remove barriers to facilitate coordination and cooperation between organizations focused on cybersecurity.
- **Legal frameworks.** Governments are charged with defining and enforcing a well-defined legal framework that clarifies responsibilities, protects participants, and reduces the attractiveness of criminal activity by providing consequences for bad actors.
- **Information sharing.** Government policy can encourage and help facilitate sharing of data between interested parties—internationally and nationally. CERTs, ISPs, software vendors, service providers, and users can all benefit from robust and efficient sharing of security-related information.

Software Suppliers

Software suppliers carry the responsibility of creating code designed with security built in from the ground up. This helps to reduce the likelihood of criminals exploiting vulnerabilities as a vector for malware installations.

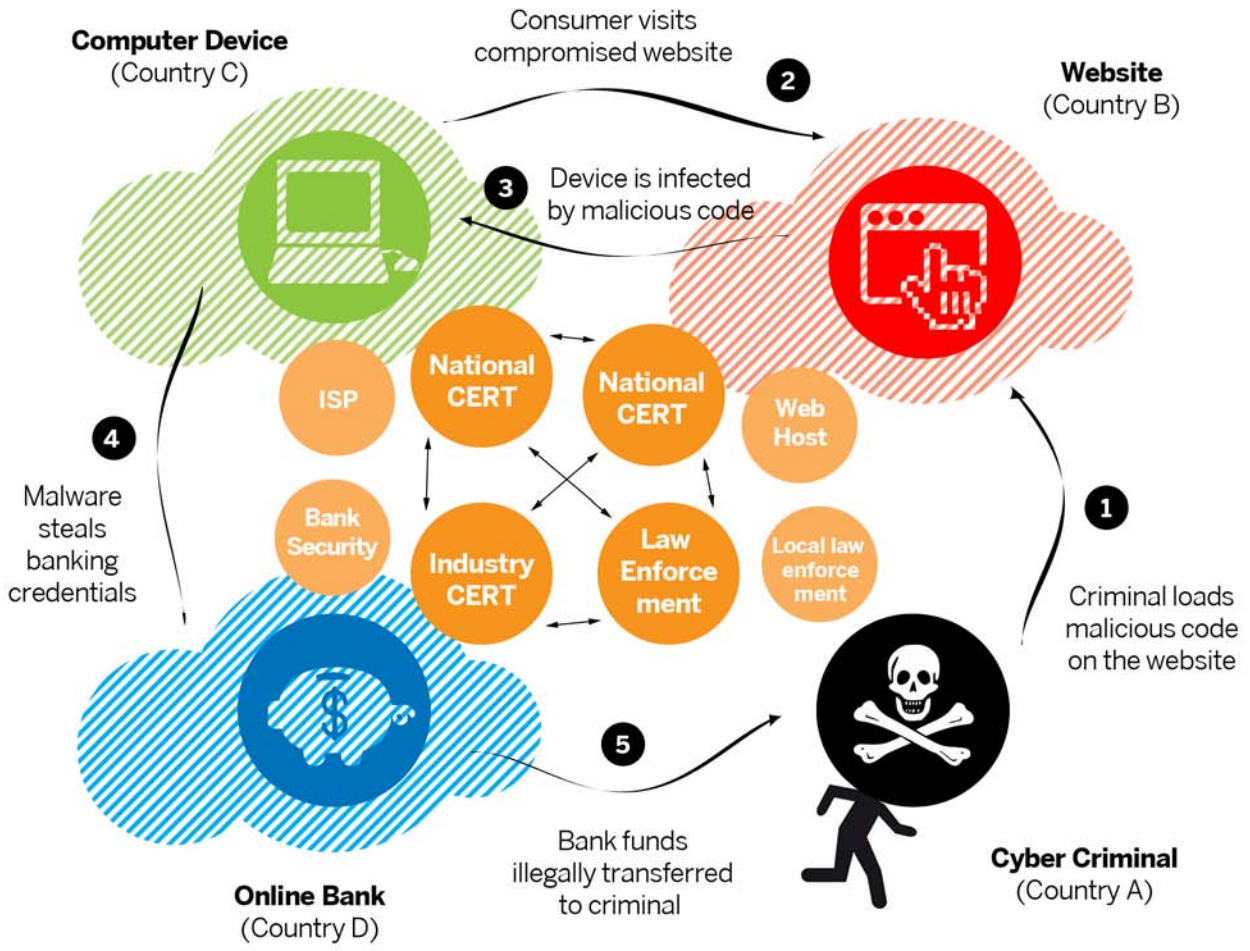


Figure 1. Anatomy of a cybercrime

Specific roles for software vendors include:

- developing products in accordance with a secure development process;
- maintaining and enhancing the security of products through rapid response to vulnerabilities and distribution of updates; and
- as appropriate, creating and distributing effective remediation tools to undo the effects of malware while preserving user data.

Internet Service Providers

ISPs are in a position to enhance security across the Internet by notifying their subscribers with infected devices and connecting them with resources to remediate the issue and prevent reoccurrence. In the past several years we have observed several positive ISP-focused activities including:

- In Australia, the Internet Industry Association in conjunction with the Minister for Broadband, Communications and the Digital Economy launched a voluntary code of practice for Australian ISPs to ensure consistent notification and remediation of consumer computer problems created by botnets. According to the code of practice, once notified of a botnet infection, the consumer is sent to a website with information to help with the cleanup.
- In Germany, the Anti-Botnet-Advisory Centre facilitates a similar arrangement with ISPs and consumers. Upon learning of the potentially compromised device, German ISPs will direct the consumer to a support resource where they receive guidance and tools for remediation.

To improve Internet health, consumers must be aware of the risks faced online, keep their devices and software up to date, and respond promptly to notifications of compromised devices or accounts.

- In the United States, the Federal Communications Commission (FCC) issued the recommendations from its Communications Security, Reliability and Interoperability Council (CSRIC) which included a voluntary U.S. Anti-Bot Code of Conduct for Internet Service Providers (Anti-Bot Code). Under the Anti-Bot Code, ISPs agree to educate consumers about the botnet threat, take steps to detect botnet activity on their networks, make consumers aware of botnet infections on their computers, assist consumers whose computers are infected, and collaborate with other service providers that have also adopted the Anti-Bot Code.

- The United States Commerce Department conducted a Request for Information (RFI) on collective industry action to address botnets in late 2011 that has led to the formation of an Industry Botnet Group that is looking at the role of the collective ecosystem to address botnets.

- Several leading ISPs around the world have individually taken great efforts to help protect consumers against botnets.

An example of a recent breakthrough in international cooperation is the EastWest Institute and Internet Society of China's track 2 bilateral effort on cybersecurity that produced the "Fighting Spam to Build Trust" report. The report's two recommendations and 46 best practices, if implemented, would help close gaps on an international level that are often exploited by malicious agents. The implementation of this report's guidance is well underway, advancing to a multilateral scale and being championed by the Message Anti-Abuse Working Group (MAAWG), which is extending the new cooperation to include botnet and mobile concerns.

Online Services

Online service providers, such as banks, e-commerce sites and social networks, can also play a role in helping consumers defend against botnet and related malware threats. The tools and techniques for detecting and notifying impacted consumers may differ from ISPs, but online service providers also have a unique channel to communicate with users. User reception of notices from service providers in the context of a financial transaction may be improved compared to an unexpected service notice. However, more research is necessary to determine the most effective means to deliver notifications.

Consumers

Consumers, ultimately, must take responsibility for the safe and secure operation of their computing devices. However, they should be supported by the vendors and service providers that they interact with online. To improve Internet health, consumers must be aware of the risks faced online, keep their devices and software up to date, and respond promptly to notifications of compromised devices or accounts.

The Internet health model requires deliberate and careful collaboration among the stakeholders mentioned above and many others. No single entity can mitigate malware threats alone, but the exact roles and responsibility between entities are still being resolved. Regardless, as more efforts such as these emerge around the world, the collective defense efforts to build a safer Internet will grow.

Establishing Metrics, Measurement and Information Sharing Schemes

One goal of implementing a public health model for cyberspace should be to involve concerned parties in states around the globe. To unify efforts across a disparate collection of organizations, ranging from national governments and CERTs to ISPs, software manufacturers, services providers, the research community and a range of public-private partnerships will need to agree upon shared metrics and measurements. Such efforts may begin with basic questions such as:

- How do we consistently measure the number of infected devices?
- What does a healthy end user device look like?
- When we apply these metrics to measure health, what do they tell us about where we are today, compared to where we have been and where we need to be in the future?

Epidemiology, a cornerstone of public health research, identifies distribution and determinants of health-related states or events, which in turn can guide policy decisions and evidence-based medicine. From the epidemiological standpoint, metrics and measurements will be essential for monitoring moment-to-moment Internet health. They can enable a better understanding of what represents traffic variants and markers that could provide early warning of malware or other threats to cybersecurity. Metrics are also critical to develop market signals for end users as to which service providers are performing better in terms of security. This strengthens the incentives of providers of all kinds to improve the security of their services.

Information sharing efforts to combat malware on end user devices have two key areas of concern: quality information and entities that are able to act upon the data they receive. Information sharing on a local and global scale will enable concerned parties to better respond to specific incidents, while aggregating data in order to develop evidence-based proactive and reactive measures to enhance overall Internet health. Currently researchers work with only small pieces of the puzzle, most often the symptoms, resulting in reactive research. Sharing cybersecurity data, like public health data, with a strong emphasis on privacy can engender research that looks globally, systemically, and more predictably at a given security problem. It is important to recognize that the CDC has in fact been able to accomplish first-class research and achieve information sharing while successfully dealing with privacy issues. Furthermore, a cyber-epidemiology approach

Currently researchers work with only small pieces of the puzzle, most often the symptoms, resulting in reactive research.

Through proactive efforts the Internet health community can enhance awareness, educate consumers, and thus promote the health of the Internet.

will promote new levels of quality research and analysis. A well-maintained repository of information with appropriate controls on access can foster trusted collaboration among participants.

Achieving such enhanced situational awareness of security threats and information sharing will require continued research on network traffic and data. The ability to detect malicious markers that are invariant, such as behavioral based indicators (e.g. insider threats) will enable a more proactive response. To facilitate innovation, richer data needs to be shared with the research community, not only incident data itself, but also datasets that will enable an understanding of what "normal" looks like. Currently, the community does not have a clear understanding of what this dataset would look like. If situational awareness is to develop beyond simple indicators, regulatory frameworks must allow access to everyday data so investigators can begin to recognize what data elements are important. This data sharing can start with limited access to high-fidelity datasets for researchers so that data with scientifically proven value is considered for sharing. Otherwise, policymakers and experts are left to speculate on what is the right data to share. To further improve the future efficiency and effectiveness of incident response, the community also needs to develop and use automated tools and techniques to analyze and correlate the vast amount of log files, artifacts, and other event information.

Moreover, compliance-driven information sharing will only lead to the bare minimum disclosure of sensitive information related to problems, concerns, and vulnerabilities. Building trusted relationships with stakeholders becomes essential to avoiding such limited information exchange and is a fundamental ingredient to a successful response. We also have to trust the people in the field and those who first respond to incidents. The application of knowledge to a practice has multiple components, including timely information distribution, dissemination, adoption, implementation, scalability, and sustainability. An increase in the application of security science to preparedness and response will prove invaluable in the long-term battle against cyber threats.

Evaluating Policy and Technology for Treating Malware and Promoting Hygiene

The remediation of devices infected with malware can be complex and burdensome. The Internet health model seeks to make remediation as easy for the user as possible, and make it easy for service providers and other involved parties to facilitate remediation. Open interoperability and security standards that allow enhancements tend to move the community in the right direction. Our hope is for a rich ecosystem of simplified, highly automated, and efficient solutions for mitigating compromised devices.

We also believe that some common guidance—perhaps driven by consumer organizations, a broad collection of ISPs, software vendors, online service providers, or CERTs—can be effective in creating a clear remediation process. The exact solutions will differ by nature of infection, technology, response programs in place, business models, and existing customer relationships. However, we believe that some uniformity of approaches can make it easier to distribute remediation efforts across the ecosystem. For example, if every vendor or service provider handles remediation differently, it may be more difficult to coordinate efforts.

Returning to the metaphor of the public health model, the difference between proactive and reactive efforts is the difference between promoting good health (e.g. hand washing) and treating disease. We must not stop our efforts at efficiently treating disease as described above. Through proactive efforts the Internet health community can enhance awareness, educate consumers, and thus promote the health of the Internet.

This raises an important question: What constitutes good health in cyberspace and how is it measured? We believe the general good health of cyberspace is produced by the consistent and ubiquitous application of technical measures combined with global political, social, and economic forces that can help thwart the highest priority threats. Measurement of device health is a topic that requires further research and investigation. Areas of interest include:

- Prescribed wellness activities for users and devices alike must be based on practices that have proven effective.

- As with human beings, a device's health is measured on a spectrum. While today we may deem a device to be infected or compromised, we will need to make more granular assessments of health in the future. When other services and devices are making decisions based on device health, the description of health will need to be more detailed than our current assessment.

- We need to better understand how to enable consumers to opt-in for self-service or professional help in managing the health of their device vs. having a broader system of health checks for devices.

- Today, many consumers make their own risk management decisions for their interactions online. Would promoting device health in a systematic manner take the consumer out of some of those decisions? If so, who would be responsible for determining the health requirements for devices?

- What is the impact of a device being considered unhealthy? How will users be protected against losing access to critical online services?

Conclusion

An Internet health system should help protect consumers and devices and provide guidance, tools, and support.

The public health model, applied in accordance with the Internet health principles in this paper, can be broadly applied to meet a range of cybersecurity challenges. While individuals today must take the ultimate responsibility for a safe online experience, they cannot solve security problems alone. Specifically an Internet health system should help protect consumers and devices and provide guidance, tools, and support to keep their devices secure and to recover from the effects of a malware infection.

Beyond the health of individual devices, promoting wellness consists of the universal advocacy and employment of proven technical measures and social pressures against the theft, loss, and destruction of personal property including one's identity. Promoting wellness includes the regular use of technical measures, good practices (e.g. to counter social engineering), and supportive services (e.g. from banks, businesses, and ISPs) needed to transform today's cyberspace into a less dangerous and more stable, convenient, and productive environment for communication, collaboration, and commerce.

	Summary of Research Focus Areas
1	Examine and address consumer expectations about security, privacy, and user control to enhance consumer participation in Internet security.
2	Determine how to embed targeted education and awareness opportunities into scam-resistant communications between service providers and consumers.
3	Further explore the necessary roles and responsibilities between ecosystem entities to determine which are best suited to provide specific Internet health functions.
4	Establish effective metrics, measurement, and information sharing schemes.
5	Explore the attributes of good health on the Internet, how that is measured, and who sets these standards.

APPENDIX

Breakthrough Group at Second Worldwide Cybersecurity Summit

The ideas in this paper are the result of nearly one year of discussions that began at the East-West Institute's Second World Wide Cybersecurity Summit held in London June 1–2, 2011. The session leaders and a summary of the discussion are included below.

Session Leaders

Co-Chairs:	**Scott Charney**, Microsoft, and **Bryan Littlefair**, Vodafone
Facilitators:	**Dr. Gregory Shannon**, CERT at CMU, and **Angela McKay**, Microsoft
Chief Editor:	**Dr. Luis Kun**, CHDS at U.S. National Defense University
Spokespeople:	**Mark Hughes**, BT, and **Jeff Jones**, Microsoft

Session Summary

The breakthrough group focused on "Collective Action to Improve Global Internet Health" met for two back-to-back sessions. The group, chaired by Scott Charney of Microsoft and Bryan Littlefair of Vodafone, consisted of nearly 30 subject matter experts from across industry, government, and academia.

Scott Charney tasked the group to take this complicated problem and decompose it into workable parts. Focusing on the problem statement, "there is currently no global, coordinated approach to protecting people from malware and related threats," the group spent the first session looking at the opportunities and limitations the public health model offered as a potential solution or inspiration to a solution for this problem.

To begin, the public health model works at all levels from the microbial to world populations. This is necessary for Internet health as well to represent all components and stakeholders. The public health model also suggests certain roles for stakeholders such as individuals, medical providers and governments. There are several areas where the metaphor does not perfectly map that will need to be addressed, including the speed of disease progression, the lack of an immune system for the Internet, and the lack of discrete populations.

The group then looked at several successful initiatives from around the world including national-level cleanup programs in Asia and Europe as well as ISP botnet notification programs in the US. The consensus was that much could be learned from these programs and shared broadly to replicate around the world.

There was also a robust discussion around metrics and measurement. The group will need to reconcile measurements at the device level with those that look at entire populations, as both will likely be valuable to different stakeholder groups. There is a sense that some short-term progress can be made in this area with an opportunity for thorough academic research on the root causes of Internet "disease" and proper data models.

EWI Board of Directors

OFFICE OF THE CHAIRMEN

Francis Finlay (U.K.)
Co-Chairman
EastWest Institute
Former Chairman
Clay Finlay LLC

Ross Perot, Jr. (U.S.)
Co-Chairman
EastWest Institute
Chairman
Hillwood Development Co. LLC
Board of Directors
Dell Inc.

Armen Sarkissian (Armenia)
Vice Chairman
EastWest Institute
President
Eurasia House International
Former Prime Minister of Armenia

OFFICERS

John Edwin Mroz (U.S.)
President, Co-Founder & CEO
EastWest Institute

Mark Maletz (U.S.)
Chair of the Executive Committee
EastWest Institute
Senior Fellow
Harvard Business School

R. William Ide III (U.S.)
Counsel & Secretary
EastWest Institute
Partner
McKenna Long & Aldridge LLP

Leo Schenker (U.S.)
Treasurer
EastWest Institute
Senior Executive Vice President
Central National-Gottesman Inc.

MEMBERS

Martti Ahtisaari (Finland)
Former Chairman
EastWest Institute
2008 Nobel Peace Prize Laureate
Former President of Finland

Tewodros Ashenafi (Ethiopia)
Chairman & CEO
Southwest Energy (HK) Ltd.

Jerald T. Baldridge (U.S.)
Chairman
Republic Energy Inc.

Sir Peter Bonfield (U.K.)
Chairman
NXP Semiconductors

Peter Castenfelt (U.K.)
Chairman
Archipelago Enterprises Ltd.

Maria Livanos Cattaui (Switzerland)
Former Secretary-General
International Chamber of Commerce

Mark Chandler (U.S.)
Chairman & CEO
Biophysical

Angela Chen (U.S.)
Founder and Managing Director
Global Alliance Associates
Partner
Epoch Fund

Michael Chertoff (U.S.)
Co-founder & Managing Principal
Chertoff Group

Ikram ul-Majeed Sehgal (Pakistan)
Chairman
Security & Management Services Ltd.

Kanwal Sibal (India)
Former Foreign Secretary of India

Henry J. Smith (U.S.)
CEO
Bud Smith Organization Inc.

Pierre Vimont (France)
Executive Secretary General
European External Action Service
Former Ambassador
Embassy of the Republic of France in Washington, D.C.

Alexander Voloshin (Russia)
Chairman of the Board
OJSC Uralkali

Zhou Wenzhong (China)
Secretary-General
Boao Forum for Asia

NON-BOARD COMMITTEE MEMBERS

Laurent Roux (U.S.)
Founder
Gallatin Wealth Mangement, LLC

Hilton Smith, Jr. (U.S.)
President & CEO
East Bay Co., LTD

CO-FOUNDER

Ira D. Wallach* (U.S.)
Former Chairman
Central National-Gottesman Inc.
Co-Founder
EastWest Institute

CHAIRMEN EMERITI

Berthold Beitz (Germany)
President
Alfried Krupp von Bohlen und Halbach-Stiftung

Ivan T. Berend (Hungary)
Professor
University of California, Los Angeles

Hans-Dietrich Genscher (Germany)
Former Vice Chancellor & Minister of Foreign Affairs

Donald M. Kendall (U.S.)
Former Chairman & CEO
PepsiCo. Inc.

Whitney MacMillan (U.S.)
Former Chairman & CEO
Cargill Inc.

DIRECTORS EMERITI

Jan Krzysztof Bielecki (Poland)
CEO
Bank Polska Kasa Opieki S.A.
Former Prime Minister of Poland

Emil Constantinescu (Romania)
President
Institute for Regional Cooperation and Conflict Prevention (INCOR)
Former President of Romania

William D. Dearstyne (U.S.)
Former Company Group Chairman
Johnson & Johnson

John W. Kluge* (U.S.)
Former Chairman of the Board
Metromedia International Group

Maria-Pia Kothbauer (Liechtenstein)
Ambassador
Embassy of Liechtenstein to Austria, OSCE and the UN in Vienna

William E. Murray* (U.S.)
Former Chairman
The Samuel Freeman Trust

John J. Roberts (U.S.)
Senior Advisor
American International Group (AIG)

Daniel Rose (U.S.)
Chairman
Rose Associates Inc.

Mitchell I. Sonkin (U.S.)
Managing Director
MBIA Insurance Corporation

Thorvald Stoltenberg (Norway)
President
Norwegian Red Cross

Liener Temerlin (U.S.)
Chairman
Temerlin Consulting

John C. Whitehead (U.S.)
Former Co-Chairman
Goldman Sachs
Former U.S. Deputy Secretary of State

* Deceased

Founded in 1980, the EastWest Institute is a global, action-oriented think-and-do tank. EWI tackles the toughest international problems by:

Convening for discreet conversations representatives of institutions and nations that do not normally cooperate. EWI serves as a trusted global hub for back-channel "Track 2" diplomacy, and also organizes public forums to address peace and security issues.

Reframing issues to look for win-win solutions. Based on our special relations with Russia, China, the United States, Europe and other powers, EWI brings together disparate viewpoints to promote collaboration for positive change.

Mobilizing networks of key individuals from both the public and private sectors. EWI leverages its access to intellectual entrepreneurs and business and policy leaders around the world to defuse current conflicts and prevent future flare-ups.

The EastWest Institute is a non-partisan, 501(c)(3) nonprofit organization with offices in New York, Brussels and Moscow. Our fiercely guarded independence is ensured by the diversity of our international board of directors and our supporters.

EWI New York Center
11 East 26th St.
20th Floor
New York, NY 10010
1-212-824-4100

EWI Brussels Center
Rue de Trèves, 59-61
Brussels 1040
32-2-743-4610

EWI Moscow Center
Bolshaya Dmitrovka St. 7/5,
Building 1, 6th Floor
Moscow 125009
7-495-2347797

EWI Washington Office
1069 Thomas Jefferson St. NW
Washington, DC 20007
1-202-492-0181

www.ewi.info