



Collective Defense

Applying Public Health Models to the Internet

By Scott Charney*
Corporate Vice President
Trustworthy Computing
Microsoft Corp.

*This paper benefited from many reviewers who provided substantive comments and helped to shape it. Please see Appendix A for admittedly incomplete list of contributors.

© 2010 Microsoft. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

Contents

The Internet—A Global Shared Domain 2

The Threat to Internet Security 2

Responding to the Cyber Threat—New Collective Defense Efforts 3

Adopting a Public Health Model for Internet Security 4

Building a Sustainable Model that Balances Security and Privacy..... 7

Shared Principles for Progress 9

Conclusion..... 10

Appendix A..... 11

The Internet—A Global Shared Domain

The Internet continues to grow at an almost unprecedented rate—connecting people, stimulating ideas, and enabling innovation for consumers, enterprises, and governments. The small number of users in the 1990's has grown to over 1.96 billion in 2009¹ and that number will continue to increase for years to come. This growth is enabled by increases in bandwidth and a proliferation of computing devices. For example, it is estimated that there will be 500 million broadband subscribers worldwide by the end of 2010² and the International Telecommunications Union has reported that mobile phone usage increased from 12 percent to 61 percent between 2000 and 2008, with a growing demand for smart phones.³ Along with this increased connectivity and a growing number and diversity of devices such as smart phones, netbooks, and e-readers, the computing model is shifting to one dependent on “anywhere access” and remote datacenters (that is, “the cloud”). Cloud computing can create efficiencies for organizations to customize and rapidly scale their IT systems, provide expanded access to computational capabilities previously available only to the very largest global companies, enable collaboration through “anywhere, anytime” access to IT for users located around the world, and promote innovation as developers take advantage of this latest computing paradigm. For governments in particular, cloud computing offers potential productivity increases and cost reduction in a time of economic constraint.

The growth in new users and devices, the richness of data being created or stored by users, and the volume of transactional data generated as a byproduct of computing activity produces valuable targets for attack. Governments and enterprises have made progress in mitigating the risk of these attacks through the development of cyber security policies and the implementation of effective security practices. By contrast, those with fewer expert resources to devote to computer security issues (such as consumers and small businesses⁴) remain challenged by malicious actors in cyberspace.

The Threat to Internet Security

Cyber threats and attacks on users are difficult to characterize and respond to for seven reasons:⁵

1. There are many different malicious actors.
2. These actors have many different motives.
3. The attacks look similar, so the nature of the attack does not always help to identify the actor and the motive.
4. The Internet is a shared and integrated domain. It is shared by individuals, organizations, and nation states and used by these groups for many different activities which cannot easily be

¹ Internet World Stats, Usage and Population Statistics. Miniwatts Marketing Group. October 1, 2010

<<http://www.internetworldstats.com/stats.htm>>.

² Research and Markets. Research and Markets. October 1, 2010

<http://www.researchandmarkets.com/research/f0e7ce/global_key_telecom>.

³ International Telecommunications Union. ITU External Affairs and Corporate Communication Division. October 1, 2010

<http://www.itu.int/newsroom/press_releases/2008/29.html> and <<http://www.itu.int/net/itunews/issues/2010/03/09.aspx>>.

⁴ Consumers and small businesses are similar in the sense that they often lack security expertise and access to expert computer security personnel. Hereinafter, the term “consumer” is used to refer to both consumers and small businesses.

⁵ For a fuller description of this issue, see the author's prior work, Scott Charney. *Rethinking the Cyber Threat – A Framework and Path Forward* May 2010, available at Microsoft Download Center. Microsoft Corporation. October 1, 2010

<<http://www.microsoft.com/downloads/en/details.aspx?FamilyID=062754cc-be0e-4bab-a181-077447f66877&displaylang=en>>.

That original paper listed six reasons that cyber threat is challenging to address but, upon further reflection, it is clear that “speed of attack” presents a seventh unique IT-related challenge.

distinguished from one another (for example, a packet may contain malware or political speech). In addition, it is hard to tease apart the different actors and activities. For instance, it is hard to monitor only the packets of individuals engaged in certain activities without in any way observing other actors and activities.

5. The speed of attack may overwhelm response methods that require human interaction.
6. The potential consequences of an attack can be hard to predict.
7. The worst-case scenarios are alarming.

It is also important to understand that most countries have already established organizations that deal with problematic conduct, including malicious Internet activity, and that these organizations often use different agencies with differing levels of authority and effectiveness, depending on who is attacking and the reasons for the attack. Yet, the “who” and “why” are often unknown when a system is under attack, which can make response challenging. Identifying cyber criminals will reduce, but not eliminate, some of the uncertainty regarding attack response. And while attribution will never be perfect, with improved attribution, cyber threats can be broken down into specific categories that will help determine what an appropriate response may be. Those categories include:

- Cybercrime.
- Economic espionage and other activities where actors may disagree on the appropriateness of particular conduct.
- Military espionage.
- Cyber warfare.

Responding to the Cyber Threat—New Collective Defense Efforts

A spectrum of actions can be taken to defend against cyber threats, even if the source of the threats cannot be specifically attributed. These activities can generally be categorized as 1) individual defense, 2) collective defense, 3) active defense,⁶ and 4) offense. This cyber defense spectrum ranges from the simplest and least controversial (individual defense) to increasingly challenging and complex responses (offense). For example, individual defense involves a single point of control (such as a person, company, or government organization) engaging in activities that affect its own assets (such as installing firewalls, running intrusion detection systems, and restricting access to information), so there is generally no objection to such activities—an entity can always raise its own defenses. By contrast, collective defense may require coordination across multiple points of control and the sharing of sensitive or even legally protected information. Some active defenses, and certain offensive actions, are more contentious because those activities may directly affect third parties, including innocent third parties who have not knowingly engaged in any malicious activities. For example, an offensive action could disable a machine infected with malware, but that infection may be unknown to the machine’s owner. Additionally, such activities may have impact beyond an actor’s sovereign border, thus raising international concerns.

As cyber security has matured over the past ten years, individual defenses in cyberspace, such as firewalls, antivirus, and automatic updates, have become more commonly available and more commonly used. While advances in technology and deployment have helped to mitigate risk in

⁶ “Active defense” refers to activity that is designed to actively interdict attacks. Indeed, some government agencies around the world are beginning to counter intrusions in real time with the goal of mitigating the impact and increasing the resiliency of enterprise operations. The limits of “active defense”, however, remain unclear. While dropping attacking packets at an upstream router may not cause harm to anyone else, one can envision active defenses that more dramatically neutralize an attacking party. In the physical world, for example, active defense might include shooting down a missile in flight before it reaches its intended target or shooting down an attacking plane with anti-aircraft fire, killing its pilot.

government and enterprise networks, it has proven insufficient for consumers and small businesses. For various reasons, the awareness and availability of security products does not always result in their deployment and maintenance and, ultimately, results in inadequate risk management. As a result, society needs to explore ways to implement collective defenses to help protect consumers who may be unaware that their computers have been compromised, and to reduce the risk that these compromised devices present to the ecosystem as a whole.

There are numerous international, national, and private sector efforts to promote or use collective defense that have had varying degrees of effectiveness. Some examples include:

- The International Telecommunications Union's (ITU) Botnet Mitigation Tool Kit raises awareness of the threats posed by botnets and documents policy, technical and social aspects that member states can use to help mitigate the effects of botnets.⁷
- Japan's Cyber Clean Center (CCC) is an example of an organized, coordinated collective defense program implemented at the national level to fight the problem of botnet infection. Based on cooperation with over 70 Internet Service Providers (ISPs), Japan's CCC promotes the cleaning of infected machines functioning as part of a botnet by contacting users and providing security software to prevent re-infection.⁸
- Signal Spam is a public-private partnership initiated by the government that collects spam reports from users and shares them with law enforcement and civil authorities, as well as major email providers, ISPs, and senders, to help remediate the root cause of spam, which is often a computer compromised by a botnet.⁹
- The Finnish national Computer Emergency Response Team, CERT-FI, runs an aggregation service, AutoReporter, that automatically compiles malware and information on security incidents related to Finnish networks and reports them to network owners. This data can be acted upon by network owners, including ISPs, to notify users of compromised devices.¹⁰
- Project MARS (Microsoft Active Response for Security) works with academic and industry experts, and utilizes technical and legal efforts in an attempt to defeat botnets. For example, the Waledac botnet was shut down through successful legal action, and then Microsoft began working with ISPs and Computer Emergency Response Teams (CERTs) to help customers remove the Waledac infection from their computers.¹¹

All of these efforts share a common commitment to help protect consumers and improve Internet health using individual and collective defenses. While each contributes to improving cyber security, these efforts have natural limitations. The reason is, in part, that end user devices not covered by these efforts are not kept up to date, rigorously checked for infections, nor are the response processes automated. As the Internet grows with new users, devices, and applications, new thinking and expanded approaches need to be applied to combat cyber threats.

Adopting a Public Health Model for Internet Security

To address cyber threats generally, and botnets in particular, governments, industry and consumers should support cyber security efforts modeled on efforts to address human illnesses. The public health

⁷ International Telecommunications Union. ITU BDT Support. October 1, 2010 <<http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html>>.

⁸ Cyber Clean Center. Cyber Clean Center. October 1, 2010 <https://www.ccc.go.jp/en_index.html>.

⁹ Signal Spam. Monsieur Jean-Christophe Le Toquin. Signal Spam. October 1, 2010 <<http://www.signalspam.fr>>.

¹⁰ CERT-FI. CERT-FI. October 1, 2010 <<http://www.cert.fi/en/reports/statistics/autoreporter.html>>.

¹¹ The Official Microsoft Blog. 8 September 2010. Microsoft Corporation. October 1, 2010 <http://blogs.technet.com/b/microsoft_blog/archive/2010/09/08/r-i-p-waledac-undoing-the-damage-of-a-botnet.aspx>.

model relies upon several core concepts that can be applied to Internet security. For a society to be healthy, its members must be aware of basic health risks and be educated on how to avoid them. Common practices to limit the propagation of disease range from the simple (washing hands) to the systematic (in schools, students may be required to be vaccinated before admission; warned if other students show symptoms; required to stay at home if infected; and notified and required to meet specified criteria for re-admission to school). In the physical world, there are also international, national and local health systems that identify, track, and control the spread of disease including, where necessary, quarantining people to avoid the infection of others.¹² To improve the security of the Internet, governments and industry could similarly engage in more methodical and systematic activities to improve and maintain the health of the population of devices in the computing ecosystem by promoting preventative measures, detecting infected devices, notifying affected users, enabling those users to treat devices that are infected with malware, and taking additional action to ensure that infected computers do not put other systems at risk.

Enterprise IT departments (including those in government organizations) have professional staff to help do this already. They often have Chief Information Officers, Chief Security Officers, professional IT staff, incident response teams, employee education and training, tools to inspect machines, and processes to ensure that devices that do not meet security health requirements are made compliant. By contrast, consumers have no such support. Moreover, many consumers have no desire to become IT professionals, let alone security experts, and information technology can be so complex that knowing how to protect oneself online is not intuitive. As a result, many consumers may be unwittingly running malware and their computers may be part of a botnet. Such botnets may be used to send spam and engage in illegal activities, including launching denial of service attacks against critical infrastructures. Some of these activities create enough traffic on the network to make other egregious activity harder to detect and mitigate. Against that backdrop, it is clear that the ability to deal with infected consumer devices generally—and botnets in particular—is an important part of any computer security strategy, including strategies to protect critical infrastructures.

The challenge of dealing with cyber crime is how do to so in a meaningful way. For years, governments, the IT industry, and concerned citizen groups have engaged in myriad activities designed to help consumers manage security risks. For example, they have been working to educate users about common threats and how to mitigate them, providing actionable advice regarding firewalls, antivirus software, and patching. Tools have been built to automatically scan devices, patch programs, update virus signatures, and remove malware when it is found. As helpful and educational as these tools are, for a host of reasons they have proven to be inadequate to prevent botnets. Some consumers do not follow the guidance provided or engage in other unsafe actions, such as downloading files from unknown sources, leading to a large number of devices becoming and remaining infected. In addition, even diligent consumers are challenged by persistent, well-funded, and more technically adept adversaries who are intent on targeting an increasing number and diversity of devices. Although addressing these threats in any context is a challenge, we need a better process of ensuring the health of the IT ecosystem. Simply put, we need to improve and maintain the health of consumer devices connected to the Internet. This will benefit not only users, but also the IT ecosystem as a whole. To realize this vision,

¹² On the international level, the World Health Organization tracks the evolving infectious disease situation, sounds the alarm when needed, shares expertise, and mounts the kind of response needed to protect populations from the consequences of epidemics, whatever and wherever might be their origin. See World Health Organization. World Health Organization. October 1, 2010 <<http://www.who.int/csr/alertresponse/en/>>. Individual countries utilize that system and may require the certain actions to treat individuals. In the United States, the Centers for Disease Control is the responsible U.S. Government agency. See Centers for Disease Control and Prevention. Centers for Disease Control and Prevention. October 1, 2010 <<http://emergency.cdc.gov/preparedness/quarantine/>>.

governments, the IT industry and Internet access providers should ensure the health of consumer devices before granting them unfettered access to the Internet.

Device health can be determined through two complementary approaches: 1) bolstering efforts to identify infected devices and 2) promoting efforts to better demonstrate device health. Bolstering efforts to identify infected devices involves analyzing and sharing data from sinkholes, network traffic, and product telemetry to identify potentially infected devices. If a device is known to be a danger to the Internet, the user should be notified and the device should be cleaned before it is allowed unfettered access to the Internet, minimizing the risk of the infected device contaminating other devices or otherwise disrupting legitimate Internet activities. In most cases, this can be done with current technology across multiple systems and platforms. In fact, at least one access provider is now attempting this approach.¹³ It is our view that approaches like this need to be broadened significantly, even globally.

Promoting efforts to better demonstrate device health can be done by granting access to resources based on the health of a device; this is similar to using Network Access Protection (NAP) in enterprise environments. To achieve this for consumer devices, four developments must occur. First, we need a mechanism for devices to demonstrate their good health (that is, a way to produce a health certificate) without rendering the systems more vulnerable, less reliable, or providing a conduit for leaking private information. Second, the mechanism that produced the health certificate must be trusted (that is, infected devices should not have a way to fake a health certificate).¹⁴ Combining trusted software such as hypervisors and hardware elements such as a Trusted Platform Module (TPM) could further enable consumer devices to create robust health certificates and ensure the integrity of user information.¹⁵ Third, access providers and other organizations must have a way to request health certificates and take appropriate action based upon the information provided. Finally, we will need to create supporting policies and rules to ensure the effectiveness of this model.

Under this model, a consumer machine seeking to access the Internet could be asked to present a “health certificate” to demonstrate its state. Although the conditions to be checked may change over time, current experience suggests that such health checks should ensure that software patches are applied, a firewall is installed and configured correctly, an antivirus program with current signatures is running, and the machine is not currently infected with known malware.¹⁶ If the health certificate

¹³ See PCMAG.COM. October 8, 2009. Ziff Davis, Inc., October 1, 2010 <<http://www.pcmag.com/article2/0,2817,2354001,00.asp>>. and CNET. September 30, 2010. CBS Interactive. October 1, 2010 <http://news.cnet.com/8301-27080_3-20018168-245.html#ixzz1133KPVK8>.

¹⁴ To be effective, ‘health certificates’ would need to be both valid and unaltered using a trusted stack of hardware and software. For additional information on the trusted stack, see the author’s prior work, Scott Charney. *Establishing End to End Trust*, available at End to End Trust. Microsoft Corporation. October 1, 2010 <<http://www.microsoft.com/mscorp/twc/endtoendtrust/>>.

¹⁵ In the long term, ensuring the trustworthiness of health certificates might require a virtual machine or small hypervisor that a consumer can use to verify the state of the machine health. In conjunction with the TPM, the hypervisor ensures that the software performing the health check has not been modified and can access all relevant information even in the event a user inadvertently granted malware highly privileged access. Currently, such highly privileged access, which may accidentally be granted by simply viewing a malicious web page, enables sophisticated malware to avoid detection thereafter. The hypervisor and health check can also be vetted to ensure that user information, choice, and use of the device are protected and remain entirely in user control. Further, such a system can act to prevent malware from interfering with sensitive interactions (banking, device updates) or stealing user information.

¹⁶ It remains true that the ability to identify malware or unacceptable anomalous behavior with certainty is limited. One can reduce the risk of false positives, in part, by identifying only malware with very well defined signatures, but that may reduce the effectiveness of the activity. These trade-offs will have to be considered carefully, but even if the health examination were limited to well-known malware the benefits would be significant.

indicates a problem, a range of options are available. For example, if the machine's health certificate reveals a security issue, such as a missing patch or out-of-date virus signature, the entity that requested that certificate (an ISP, for example) may provide a notice that assists the user in addressing the security concern or directs the user to resources for remediation. If the problem is more serious (the machine is spewing out malicious packets), or if the user refuses to produce a health certificate in the first instance, other remedies such as throttling the bandwidth of the potentially infected device, might be appropriate. As devices converge (like if a computer is used to make Voice over Internet Protocol (VOIP) calls), denying a user complete access to the Internet, even for a short period, could well have damaging consequences. For instance, an individual might be using his or her Internet device to contact emergency services and, if emergency services were unavailable due to lack of a health inspection or certificate, social acceptance for such a protocol might rightly wane. But much like a cell phone may require a password but still allow emergency calls to be made even without that password, infected computers may still be permitted to engage in certain activities.

There are at least two other advantages of this health certificate model. First, its use need not be limited to access providers; organizations and consumers could use these health certificates in other situations where the health of the machine may be important to all concerned (such as before online banking activities). Another advantage of health certificates is that they can be specific to a single device, thus enabling more effective remediation. For example, if a home has multiple devices, an ISP that detects suspicious network traffic may have no way of knowing which device is infected. With a health certificate, the ISP could tell the user which certificate revealed an issue and the user could then take appropriate action to improve the health of the affected device.

Building a Sustainable Model that Balances Security and Privacy

As cyber security policy and corresponding legislation is being actively discussed in many nations around the world, there is a huge opportunity to promote this Internet health model. As part of this discussion, it is important to focus on building a socially acceptable and financially sustainable model.

While the security benefits may be clear, it is important to achieve those benefits in a way that does not erode privacy or otherwise adversely impact freedom of expression and freedom of association. Ensuring users have control over health certificates and the way they can be used—and that users understand the implications of refusing to attest to good health—is an important first step in ensuring appropriate user engagement. It is important to decide, too, whether health certificates will reveal simply the state of the machine, or more about the identity of the device and, potentially, its user. Certainly, a machine could be denied unfettered access to the Internet based upon certain health attributes without determining more about the machine or its user. On the other hand, there may be value in uniquely identifying devices, as when a device may be infected on a home network. It may also be possible, of course, to combine device information with other information to identify a user (much like cell phones may have unique identifiers and can be tied to particular account holders). To what extent a health system should allow specific devices and their users to be identified cannot be resolved here, but it is important to note that a carefully architected system that embraces privacy by design, along with carefully constructed threat models that contemplate potential abuses of the health system, can help ensure the right technical and non-technical controls are in place to mitigate potential social harms and ensure the appropriate balancing of interests.

Even when health care certificates are oriented toward privacy, societies still need to agree that using them to regulate unfettered access to the Internet is a sound approach. That may depend, in part, on what the health certificate reveals, what happens when a device is out of compliance, and what happens when disputes about machine health arise. If such a program is market-driven, the terms of

service might well be governed by contracts. However, for users whose service is provided by a government, such a solution may not be so simple. Either way, governments may still want to regulate how health certificates can be used so that any program is limited to ensuring device health and that information gathered is used for no other purpose (for example, the enforcement of intellectual property rights, the creation of marketing profiles). Limiting the scope of the program to device health issues would help reduce concerns that Internet health issues were being used to justify activities not related to Internet security. A further mitigation that implementers could consider is to have an authorized third-party audit of the process used to create and present the health certificates to ensure that the technology is only identifying and reporting what it should. The European Privacy Seal (EuroPriSe) is an example of such an independent certification process.¹⁷

Whether governed by Terms of Service or regulation, individuals who have relatively unfettered access to the Internet today may still argue that any restrictions are offensive. In that regard, looking at how many nations have addressed smoking as a health related issues may be illustrative. Individuals are allowed to smoke—notwithstanding the health risks to smokers and the indirect costs on society—on the theory that individuals have a right to engage in certain potentially self-destructive activities. When the Environmental Protection Agency identified the dangers in second hand smoke, however, smoking was banned in a wide range of public places. The argument was that individuals might have the right to risk their own health but they do not have the right to injure others. One could argue that computer security is similar. Consumers have been told for years to keep their systems up to date, run antivirus programs, and backup their data. Like smokers, they were told that the failure to follow the advice given would put them at risk, but ultimately they could choose to accept that risk. With botnets and similar types of malware, however, one is not simply risking one’s own device—one is putting others at risk too. Notwithstanding the parallel, we recognize that smoking has been regulated in public places and computers may sit in the most private of places. But Internet-connected users are using a shared resource that needs to be protected for the good of others, including the protection of critical infrastructures.

Interplay also exists between this public health model and situational awareness. Information learned through the health examination process may be extremely valuable to those attempting to understand and preserve the health of the Internet. As such, it needs to be decided whether this information can be provided to others, such as the government, technology vendors, and access providers, and under what conditions. Similarly, threat and vulnerability information obtained from other sources—and in the possession of the government, technology vendors and others—may be critically important to protecting network health. As such, it will need to be decided whether threat and vulnerability information can be shared with access providers and those requesting health certificates so they can fulfill their network protection functions. Clearly, malware spreads far faster than humans can react, and rapidly sharing threat, vulnerability, and other network health information has taken on increased importance. Equally important is the ability to automate the detection and treatment process itself. Today, information is not shared for a host of reasons that have been well documented by assorted commissions and advisory committees. These issues are, if slowly and imperfectly, being addressed. But policy makers should appreciate that the ability to rapidly share computer health information will be critical to increasing the effectiveness of this model, just as sharing health information has been critical to containing human outbreaks such as SARS and H1N1.

¹⁷ The EuroPriSe European Privacy Seal for IT Products and IT-Based Services. Unabhaengiges Landeszentrum fuer Datenschutz Schleswig-Holstein (ULD). October 1, 2010 <<https://www.european-privacy-seal.eu/about-europriSe/fact-sheet>>.

Finally, society must focus on the costs of ensuring Internet health. In its report, “Securing Cyberspace for the 44th Presidency,”¹⁸ the Center for Strategic and International Studies Commission observed that the public private partnership needs to be modernized and made more effective by emphasizing more operational collaboration. The report articulated the need for the roles of industry and government to be complementary. The report specifically stated that

[I]ndustry and government should identify the level of security that market will naturally provide. Regulation would create processes to fill the gap between what markets will provide and what national security requires. The government’s tool kit for this change should be viewed as expansive and flexible, including the use of policy and economic incentives to reinforce or supplant regulation.¹⁹

Determining the required level of security for a rapidly evolving information infrastructure is not easy, yet as countries around the world plan and deploy broadband networks, there is an opportunity to help consumers meet necessary security levels. If access providers providing device health services today are successful with those services, either because reducing malware drives down network costs or because consumers are willing to pay for the service, it may be true that “market forces” are enough to drive adoption of this model. But if market forces prove insufficient, then the government should use the tools in its tool kit to ensure the model is economically viable.

Shared Principles for Progress

With security and privacy in mind, the following statements reflect the concepts outlined in this document and are intended to help guide stakeholders efforts, promote action, address challenges, and influence future initiatives.

- The risk that botnets present to Internet users and critical infrastructures must be addressed.
- Collective defense can and should be used to help improve the security of consumer devices and protect against such cyber threats.
- A public health model can empower consumers and improve Internet security.
- Voluntary behavior and market forces are the preferred means to drive action, but if these means fail, governments should ensure these concepts are advanced.
- Privacy concerns must be carefully considered in any effort to promote Internet security by focusing on device health. In that regard, examining health is not the same as examining content; communicating health is not the same as communicating identity; and consumers can be protected in privacy-centric ways that do not adversely impact freedom of expression and freedom of association.

As noted earlier, there are a few projects and initiatives underway that are reducing malware infections in their specific country or region. While helpful and consistent with these ideas presented in this paper, they are too disparate to have the effectiveness that more collective action could create. Partners across the ecosystem, including the IT industry, ISPs, and governments need to help foster greater collective defense. We can do this by bolstering efforts to identify infected devices and promoting efforts to better demonstrate device health. Device health can be improved, in part, by taking three specific steps: 1) ensuring that devices can generate trustworthy health certificates. 2) building infrastructure that allows

¹⁸ Center for Strategic and International Studies. Center for Strategic and International Studies. October 1, 2010 <<http://csis.org/publication/securing-cyberspace-44th-presidency>>. The author of this paper is a co-chair of the CSIS Commission.

¹⁹ *Id.* 50-51.

access providers and other interested parties to consume those health certificates and take action based upon the state of the device, and 3) creating policies to encourage health certificate use and ensure rapid information sharing as new threats emerge.

Collectively, we can help develop and promote the expected actions and behaviors that will improve Internet safety across the computing ecosystem. To build on the current national and industry efforts, we can identify what is working and what is not, and document both to enable more individual action and community building. We can also begin to work through international bodies to standardize what types of information on machine health should be shared and how to exchange it with appropriate security and privacy protections. As more efforts advance, we can create guidelines to catalyze further action. We must also drive the research and development that will remove barriers to, lower costs for, and incent the actions and behaviors outlined above. Finally, we can advocate for the necessary policy and legislation reform to enable and eventually transition to a state where collective defense and consumer endpoint health management is not just feasible, but a reality.

Conclusion

The rate of growth of the information society, the sophistication of threats targeting users, and the potential consequences of consumer devices being directed towards critical infrastructures requires new thinking and new collective action by the Internet community. We cannot expect consumers to become security experts, but if we think about how the public health model helps consumers to understand when they are ill and when they should get treated, we can come up with relevant concepts that are applicable to Internet security. The public health model is not perfect, nor does it need to be—where there are differences there may also be useful insights. For example, the medical model is massively distributed and has far more endpoints (doctors, nurses and pharmacists) than the computer model (there are fewer access providers than medical professionals), so IT professionals may identify critical trends more quickly. And while computer viruses may spread faster than human viruses, automation may permit devices to be vaccinated more quickly than people. Governments and industry, by focusing on the similarities and differences between the physical and the IT world can construct IT response mechanisms far more effective than what exists today.

For more information, please visit www.microsoft.com/security/internethealth.

Microsoft[®]

Appendix A

During the creation of this paper, many people were provided with drafts or heard briefings and provided extremely helpful comments. In some cases, some individuals provided cumulative comments from their teams and I do not have a complete list of reviewers. In other cases, I presented this concept at organized events and received helpful comments in hallway conversations after the event. I apologize, in advance, for failing to recognize everyone individually.

I want to thank the many people within, or affiliated, with Microsoft who provided thoughtful comments and ideas that substantially improved this paper. The list includes, but is not limited to, Jules Cohen, Jeffrey Friedberg, Cristin Goodwin, Jeff Jones, Angela McKay, Matt Thomlinson, John Manferdelli, Craig Mundie, Paul Nicholas, Kevin Sullivan and members of the Trustworthy Computing Academic Advisory Board.