Creating the Demand Curve for Cybersecurity

Melissa Hathaway

Melissa Hathaway led President Obama's Cyberspace Policy Review and previously led the development of the Comprehensive National Cybersecurity Initiative (CNCI) for President George W. Bush. She is now President of Hathaway Global Strategies LLC and Senior Advisor at Harvard Kennedy School's Belfer Center.

This article has been updated from an earlier version that was published by the Atlantic Council in December 2010. The original is available at: http://www.acus.org/files/publication_pdfs/403/121610_ACUS_Hathaway_CyberDemand.pdf

America's future economic and national security posture enabled by the digital revolution is at risk. If the Administration is serious about mitigating that risk by increasing the security of the nation's information and communications infrastructure, it should exercise every instrument of power to drive us toward a better place. With little more than one year left in this Administration, there are fewer options at hand to drive progress. The President's Fiscal Year 2012 budget is under review by Congress and maintains the status quo for funding cybersecurity programs. Further, the President's staff continues to struggle with the complex policy formulation regarding cybersecurity and are slow to make progress on the nearly two dozen recommendations set forth in the Cyberspace Policy Review. Even if policy changes were imminent, without a funding priority underpinning the initiatives, one can expect little change.

The combination of divided government and the upcoming presidential election cycle means that making progress

on its policy priorities will be challenging for the Administration. But the President has other levers of power that he could use to raise awareness of what is at stake and set us on a better path to keep our economy and our citizens secure. They would not require congressional approval; rather, they would require political resolve and determination to make dramatic change in our risk posture during the remaining term of his Administration.

The President can turn to three independent regulatory agencies for help: the Securities and Exchange Commission, the Federal Communications Commission, and the Federal Trade Commission. A strategy involving these three agencies could dramatically increase awareness of what is happening to our core infrastructure and drive an innovation agenda to strengthen our information security posture. Furthermore, this strategy could increase productivity because it will reduce the losses sustained on a daily basis by our companies and citizens.

Turning to the Securities and Exchange Commission First, the President should consider asking the Securities and Exchange Commission (SEC) to examine and evaluate a policy that would require Chief Executive Officers (CEOs) to attest to the integrity of their company's information infrastructure.[1] The SEC could open a dialogue with industry through an administrative notice to industry informing them that the SEC will consider making a rule regarding the thresholds of materiality risk in the area of information security. This notice would inform registrants that the SEC would ask management to provide an assessment of the effectiveness of the registrant's controls over the protection of proprietary and confidential personal data, mission critical systems, and their incident response and remediation capability in the event of an incident. An announcement could recognize that companies continue to face significant challenges in their ability to appropriately protect their computer systems, secure their proprietary, customer, and financial information, and safeguard the integrity of business and other transactions that they conduct over the Internet. Reports are released daily that reveal the industry losses that result from poor information security policies and porous infrastructures.

This is an area that needs greater transparency. In fact, a recent report by the Ponemon Institute disclosed that on "an annualized basis, information theft accounts for 42 percent of total external costs, and the costs associated with disruption to business or lost productivity accounts for 22 percent of external costs."[2] Many firms are resistant to public disclosure because the details of their compromises or breach may change public perception or impact customer confidence or competitive advantage.

We may, however, be at a turning point. Since the January 2010 incident involving Google, more executives are discussing the topic of information security and cybersecurity. Alan Paller of the SANS Institute announced that the Google incident actually affected more than two thousand companies.[3] In its January 2010 annual report filed with the SEC, Intel Corporation disclosed "[w]e may be subject to intellectual property theft or misuse, which

could result in third-party claims and harm our business and results of operations." The corporation's proactive self-disclosure suggests that management understands the risk assumed by the business. Can the SEC facilitate other companies to assume more pro-active measures to determine if they have been penetrated and have lost information?

Even beginning a dialogue on this issue may force companies to better understand the scope, adequacy, and effectiveness of the internal control structure and procedures for protecting their information assets (data and infrastructure), and to invest in risk mitigation actions. But if that is not enough, in its review of the quarterly and annual reports and other filings by registrants, the SEC staff could ask registrants whether they have adequately disclosed material risk to their company's protection of customer data, proprietary data, and mission critical systems and infrastructures. Separately, when assessing internal controls, auditors could assess the company's internal controls for the protection of internal financial and management data. Because if that data is not secure, how can the assessments be reliable to shareholders?

There are other attendant benefits of the SEC moving in this direction. First, it will create a national, if not international, dialogue on the extent of professional criminal activity and depth of economic espionage conducted against global corporations worldwide. Board rooms around the world will turn to the CEO, Chief Information Security Officer (CISO), Chief Information Officer (CIO), and Chief Risk Officer and ask what they are doing to improve the level of security of their infrastructure and the online environment that supports it. As material risk is discovered, reporting will result in data and statistics, and will perhaps yield a quantitative picture of the economic impact of intrusions.

This risk disclosure may also facilitate the identification of solutions to the root cause of the problem. Industry will demand industry-led innovation with a newfound sense of urgency to eliminate or mitigate the risk of reporting in the following year. Companies may turn to their Internet service providers (ISPs) to provide increased managed security services on their behalf. Concurrently, the security product industry will have an increased market-driven requirement to deliver products that perform with higher assurance levels. The research community will now also have access to data that will facilitate idea creation and innovative solutions that increase security across the entire architecture.

The increased data that will result from such risk filings may also lead to the growth of an insurance industry that will help companies to absorb costs if they show a minimum standard of due care. While some insurance companies are beginning to offer policies that are designed to protect businesses should they fall victim to intrusions or other forms of online disaster, there presently is not enough actuarial data from which to reliably base the premium rates.[4] If companies had to disclose intrusions and the associated external costs of lost intellectual property or lost productivity, insurance policies and costs would have to be more predictable.

Further, as more data becomes available, a standard of care or best practices of the enterprise could emerge. This

would allow businesses to deploy capabilities in a way that provides adequate protection, taking into account risk requirements and business operations. Then, if a corporation has implemented adequate defenses of its networks or information assets and a breach does occur (e.g., illegal copying and movement of data), it could call upon its insurance plan to supplant the losses. Of course, this will lead to a discussion on liability, and may in fact unfold the legal underpinnings associated with it.

This proposal may seem somewhat dramatic and industry may appeal the unintended consequences of implementing a rule in this area, citing high costs and reduced competitiveness. But regulators can compare this proposal to the Sarbanes-Oxley Act of 2002, which introduced major changes to the regulation of corporate governance and financial practice as a result of identified weaknesses, as illustrated by the Enron case among others. And why should the SEC not take measures to protect the near-term economic infrastructure and long-term growth of publicly traded companies?

The major telecommunications providers and ISPs, collectively, have unparalleled visibility into global networks…

Turning to the Federal Communications Commission

Together with the SEC option, the President can turn to the Federal Communications Commission (FCC) to enlist private-sector talent and require the core telecommunications companies and Internet Service Providers (ISPs) to shoulder greater responsibility in protecting our infrastructure. The major telecommunications providers and ISPs, collectively, have unparalleled visibility into global networks, which enables them with the proper tools to detect cyber intrusions and attacks as they are forming and transiting towards their targets.[5] They even have the ability to tell you, as a consumer, if your computer or network as been infected. For example, Comcast is "expanding a pilot program that began in Denver last year, which automatically informs affected customers with an e-mail urging them to visit the company's security page."[6] Customers are receiving alerts, being offered anti-virus customer service, and receiving free subscriptions to Norton security software. While these companies are only beginning to offer these tools to customers as an enhanced service, they already employ sophisticated tools and techniques for countering attacks to their own infrastructure and the networks.

So, why does the FCC not mandate that this service be provided more generally to clean up our infrastructure? Of course, this may open a dialogue or request to limit the liability for providing such a managed security service. Perhaps the "good Samaritan" clause in the Telecommunications Act of 1996 could be reviewed and applied to quell any concerns that may surface.[7]

Other countries are turning to their ISPs to ensure the health of their Internet backbone. For example, Germany has determined that the botnet infestation (large clusters of zombie computers, controlled by third parties, that can be used for cyber attacks) in its private infrastructure is a priority for national defense. As such, the German Federal Office for Information Security (BSI) has mandated that its ISPs track down infected machines and provide advice to users on how to clean their computers.[8] Similarly, Australia's ISPs have adopted a code of conduct designed to mitigate cyber threats and inform, educate, and protect their users from cybersecurity risks.[9] The European Parliament and Council of Ministers reached an agreement on pan-European telecommunications reform that will be transposed into national laws in the coming months. It obliges the ISPs to take more responsibility for providing enhanced security services to their customers and to report all security incidents to the European Network and Information Security Agency (ENISA).[10]

If the FCC were to require such a service to be implemented in the United States, it would immediately reduce the proliferation of malware and infections. Such a requirement would also focus attention and innovation toward more sophisticated threats, and would establish a baseline of security for the broad infrastructure. Further, the FCC could request that there be a reporting function associated with this service. Combining their collective network visibility would support a national warning and assessment capability, and would also facilitate a real-time exchange and consolidation of threat information and response capabilities.[11] The created information base would cut across all segments of the private and public sector, providing a good view as to where and how resources should be allocated.

Providing this type of service should be a requirement not only for the "traditional" telecommunications carriers like AT&T, Verizon, and Sprint, but for other ISPs that provide core communications services as well, such as Comcast, Cox Communications, and Time-Warner Cable. Furthermore, companies like Google, Microsoft, and Amazon should also be required to provide this type of notification or reporting for their Cloud services.

Given the rapid consumer adoption (government, industry, and citizen) of technology and the growing migration of essential services to Internet-based infrastructure, the FCC should classify broadband and other Internet services as core telecommunications. As the communications infrastructure migrates from older to newer technologies, services like energy (Smart Grid) and public safety (Voice Over Internet Protocol) will be carried over a communications network that may or may not be built to the same standards for which the traditional voice telephone system was built. The FCC realizes that it "needs a clear strategy for securing the vital communications networks upon which critical infrastructure and public safety communications rely,"[12] but is that enough? Key in this debate is the issue of preserving the open Internet while allowing network operators the flexibility and freedom to manage their networks as they provide security to our core infrastructure. Another important question is whether to hold

wireless broadband and wireline carriers to the same standard in the coming decade, when growth will be derived by wireless services and technologies.[13]

Whether wireline or wireless, the FCC must take a stance and assure that carriers contribute to the security and resiliency of our communications infrastructure. After all, it is the very service for which they have assured we will have 100 percent uptime. Why not provide it with less malware, spam, and infections? It would certainly help the companies that are under constant barrage from those trying to copy their intellectual property illegally. It would help the average consumer in taking action to address a compromised PC on the home network. And it would help the government to develop a better understanding of the malicious activity that happens inside the networks and infrastructures that are key to the nation's economic growth and security posture.

Criminal activity targeted toward consumers is a pandemic that must be addressed head on.

Turning to the Federal Trade Commission

As Secretary Locke recently stated, "each year, the world does an estimated $10 trillion of business online. Nearly every transaction you can think of can now be done over the Internet: consumers can pay their utility bills from their smart phones; nearly 20 percent of taxpayers file returns electronically; people download movies, music, books and artwork into their homes; and companies, from the smallest local store to the largest multinational corporation, are ordering their goods, paying their vendors and selling to their customers online. However, the Internet will not reach its full potential as a medium until users feel more secure than they do today when they go online."[14] This statement illustrates why the President must turn to the Federal Trade Commission (FTC) in order to engage the public on cybersecurity.

Criminal activity targeted toward consumers is a pandemic that must be addressed head on. Countries around the world are calling for action. Professional criminals are innovating and developing new ways to generate revenue from compromising our computers through scams, spam, and malicious software. They adapt to whatever information security measures are in place and rob our bank accounts, steal our credit cards, and assume our identity. The Federal Trade Commission has a broad mandate to protect consumers and to educate consumers and businesses on the fundamental importance of good information security practices. The FTC believes that companies must take the appropriate steps to protect consumers' privacy and information and that they should have a legal obligation to take reasonable steps to guard against reasonably antic-

ipated vulnerabilities. The FTC maintains a website (www.OnGuardOnline.gov) that provides practical tips from the federal government and the technology industry to help consumers and businesses to guard against Internet fraud, to secure their computers, and to protect personal information.

But this is not enough when it comes to making consumers aware of the risks associated with e-transactions. The FTC should consider a more proactive initiative and require all e-commerce transactions to carry a warning banner or label that informs consumers that they are assuming a risk by conducting e-transactions and that their transaction may not be secure and in fact could compromise their credentials. This can be compared to the tobacco label of "smoking is hazardous to your health" or the label on a bottle of wine that warns the consumer that "consumption of alcohol may cause health problems."

An e-transaction warning label may seem like a drastic step toward improving the ability of firms and consumers to keep pace with ever-evolving cybersecurity risks, but it will raise awareness for every person who executes on-line transactions. In 2009, online retail sales grew 2 percent to reach $134.9 billion, while total retail sales fell 7 percent in that same year.[15] Analysts expect this trend to continue. At the same time, security analysts see the growth of cyber crimes increasing by more than 20 percent on a year over year basis. Consumers must be aware of the risks of e-commerce, and providers have a responsibility to disclose that they are taking all necessary measures to ensure that their infrastructure is secure, at least to a minimum standard, and that they are working diligently to protect their consumers' transactions.

The FTC might also consider establishing baseline standards for conducting trusted transactions in cyberspace, such as secure encrypted envelopes, digitally signed critical information, and secure serial numbering and checking to provide more protection for online consumer transactions. They should not prescribe technical solutions per se, but rather, principles of protection.

The Commerce Department and the FTC must ensure that the Internet remains a fertile ground for an expanding range of commercial and consumer activity. They also must do a better job of raising national awareness of the forces that put consumer e-commerce activity at risk.

Conclusion If the Administration truly seeks to make cybersecurity a national priority it must move away from the tactical programs that we have seen thus far that may militarize cyberspace (e.g., creation of Cyber Command) or may create a false sense of control, privacy, and security with the National Strategy for Trusted Identities in Cyberspace. We need real leadership and bold steps. While not everyone would embrace this proposed economic triad of regulation, these initiatives would be a catalyst for change and constitute a "shot-in-the-arm" to raise awareness and boost our national cyber defense immediately. These initiatives also could signal to the international community that the United States is serious, and with the full commitment of the nation, will solve this problem.

The Administration has few tools left in the remaining year of this term. It is

a bold step to turn to the independent regulatory bodies, but it is a tool that is at the sole prerogative of the President. While these proposals may face resistance, they will spark debate and dialogue, which by itself could accelerate addressing the problem responsibly. We need to raise national awareness quickly. We can no longer afford to have a polite conversation, or worse yet, remain silent. Rather, we need to be guided by the urgency and seriousness of the situation, develop an exquisite understanding of what is at stake, and address it with good old-fashioned American ingenuity. We can create and drive an innovation agenda to strengthen our information security posture, and perhaps gain economic strength as we increase productivity. This proposal, if implemented, will create the demand curve for cybersecurity and will reduce the losses sustained on a daily basis by our companies and citizens.

NOTES

1 Melissa Hathaway published this argument in December 2010 in an Atlantic Council Issue Paper. Since the publication of her article, Senator Rockefeller sent a letter to SEC Chairman Mary Schapiro on 11 May 2011. In the letter, he asked the SEC to look into corporate accountability for risk management through the enforcement of material risk reporting. In June 2011, Chairman Schapiro said that the SEC would look into the matter.

2 Ponemon Institute, "First Annual Cost of Cyber Crime Study," July 2010

3 Alan Paller, "SANS WhatWorks in Security Architecture Summit 2010" (Las Vegas, NV, May 2010).

4 David Briody, "Full Coverage: How to Hedge Your Cyber Risk." INC., Internet, http://www.inc.com/magazine/20070401/technology-insurance.html (date accessed: 4 August 2011)

5 National Defense Authorization Act of 2011, H.R. 5136, 111th Congress, 2011.

6 Brian Krebs, "Comcast Pushes Bot Alert Program Nationwide" *Krebs on Security*, Internet, http://krebsonsecurity.com/2010/10/comcast-pushes-bot-alert-program-nationwide/.

7 The Telecommunications Act of 1996. Pub. L. No. 104-104, 110 Stat. 56. The 1996 Telecommunications Act included a "good Samaritan" provision to protect Internet Service Providers (ISPs) from liability when they act in good faith to block or screen offensive content hosted on their systems. Id. § 230(c).

8 John Leyden, "German ISPs team up with gov agency to clean up malware." *The Register*, 9 December 2009.

9 Ben Bain, "Australia Taps ISPs to Fight 'Zombies'," *Federal Computer Week*, Internet, http://fcw.com/articles/2010/06/29/web-aussie-isp-code.aspx. The code was drawn up by the Australian Internet Industry Association (IIA) in conjunction with Australia's Broadband, Communications and the Digital Economy Department and the Attorney General's Department.

10 "*Acts adopted under the EC Treaty/Euratom Treaty whose publication is obligatory*," Internet, http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2009:337:SOM:EN:HTML.

11 National Defense Authorization Act of 2011, H.R. 5136. 111th Congress, 2011.

12 The United States Federal Communications Commission, "Connecting America: The National Broadband Plan" (16 March 2010).

13 Nilay Patel, "Google and Verizon's Net Neutrality Proposal Explained," *Engadget*, Internet, http://www.engadget.com/2010/08/09/google-and-verizons-net-neutrality-proposal-explained/.

14 Commerce Department Documents and Publication. "U.S. Commerce Secretary Gary Locke Announces Initiative to Keep Internet Open For Innovation and Trade at Cybersecurity Forum," Internet, http://www.tmcnet.com/usubmit/2010/09/23/5025949.htm.

15 U.S. Census Bureau, ''Quarterly Retail E–Commerce Sales: 4th Quarter 2008,'' U.S. Census Bureau (16 Feb. 2010).