ATLANTIC COUNCIL
IDEAS. INFLUENCE. IMPACT.

ISSUEBRIEF

Melissa E. Hathaway

PROGRAM ON INTERNATIONAL SECURITY

Creating the Demand Curve for Cybersecurity

America's future economic and national security posture, enabled by the digital revolution, is at risk. If the Obama 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 at hand to move the United States toward a better place.

Nearly two years into this administration, there are fewer options available to drive progress. The President's fiscal year 2011 budget, under review by Congress, maintains the status quo for funding cybersecurity programs. Further, the President's staff continues to struggle with the complex policy formulation regarding cybersecurity, and has been slow to make progress on the nearly two dozen recommendations set forth in the administration's Cyberspace Policy Review. Even if policy changes were imminent, little would change without a funding priority underpinning the initiatives. In the absence of a push to prioritize funding, the administration needs a new approach to mitigate our nation's vulnerability to cyber attacks.

As a result of the midterm elections, the balance of power in Congress will change in January, making progress on administration policy priorities even more challenging. Nonetheless, the President does have levers of power available to him that he could use to raise awareness of what is at stake, enabling him to set the nation on a better path toward keeping our economy and citizens secure. These levers do not require congressional approval; rather, they require political resolve and determination to make dramatic changes in our risk posture during the remainder of the President's term.

The Program on International Security shapes and influences the debate on international security by facilitating dialogue through critical analysis and policy-relevant programming on the greatest security challenges facing the United States and the transatlantic community. The Program builds on the Council's extensive network of experts and practitioners in North America and Europe to inform policy and to introduce ideas into the public debate. The Program influences policy and shapes ideas by publishing task force reports and analytical issue briefs, providing a public speaking platform for leaders in international security, briefing policymakers and national security leaders in private strategy sessions, and hosting working groups to tackle the most complex challenges in international security. For more information, contact Vice President and Director of the Program on International Security Damon Wilson (**dwilson@acus.org**) or Associate Director Magnus Nordenman (**mnordenman@acus.org**).

The Program on International Security's work on cyber security issues is generously supported by SAIC.

This proposal asks the President to turn to three independent regulatory agencies for help. This three-pronged strategy could dramatically increase awareness of what is happening to our core infrastructure, drive an innovation agenda to strengthen our information-security posture, and increase productivity, as it would reduce the losses being sustained on a daily basis by our companies and citizens.

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.

Turning to the Securities and Exchange Commission

First, the President should consider asking the Securities and Exchange Commission (SEC) to evaluate the importance of requiring chief executive officers (CEOs) to attest to the integrity of their companies' information infrastructure. The SEC could open a dialogue with industry through an administrative notice, informing companies that the SEC would consider a rule regarding the thresholds of materiality risk in the area of information security. This would put registrants on notice that the SEC is likely to require more information from company management to verify the existence of proper safeguards. More specifically, the SEC would request that registrants show an ability to protect proprietary and confidential personal data, demonstrate the existence of appropriate safeguards for mission-critical systems, and explain their ability to quickly and effectively respond to a cybersecurity incident.

> "...the President should consider asking the Securities and Exchange Commission (SEC) to evaluate the importance of requiring chief executive officers (CEOs) to attest to the integrity of their companies' information infrastructure."

Such an announcement would recognize that companies continue to face significant challenges when it comes to their ability to appropriately protect their computer systems; to secure their proprietary, customer, and financial information; and to safeguard the integrity of business and other transactions they conduct over the Internet. Reports released daily reveal that significant industry losses result from poor information-security policies and porous infrastructures. This is an area that needs greater transparency. In fact, a recent Ponemon Institute report 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 account for 22 percent of external costs."[1] Many firms are resistant to public disclosure because the details of their compromises or security breaches may change public perception, or impact customer confidence or competitive advantage.

We may, however, be at a turning point. Since Google's January 2010 disclosure of Chinese-origin cyber attacks (known as Operation Aurora), more executives are discussing the topic of information security and cybersecurity. Alan Paller of the SANS Institute announced that the Google incident affected more than 2,000 companies.[2] In January 2010, Intel Corporation disclosed risk areas in its annual report filed with the SEC, noting: "We may be subject to intellectual property theft or misuse, which could result in third-party claims and harm our business and results of operations." Intel's disclosure suggests that its management understands the risk assumed by the business. Can the SEC encourage other companies to assume more proactive measures to determine whether they have been penetrated and have lost information? Simply beginning a dialogue on this issue may force companies to better understand the scope, adequacy, and effectiveness of their internal control structures, and the procedures they use to protect their information assets (data and infrastructure); better yet, this dialogue could prompt them to invest in risk-mitigation actions.

But if that is not enough, in its review of registrants' quarterly and annual reports and other filings, 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, auditors could assess the company's internal controls for the protection of internal financial and management data. After all, if that data is not secure, how can their assessments of the company's financial position be reliable to shareholders?

There are other attendant benefits that could result from the SEC moving in this direction. First, such a move would force a national (if not international) dialogue on the extent of professional criminal activity and the depth of economic espionage being conducted against global corporations worldwide. Boardrooms around the world would turn to the CEO, chief information security officer (CISO), chief information officer (CIO), and chief risk officer (CRO) to 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 would result in improved data and statistics, and perhaps yield a quantitative picture of the economic impact of intrusions.

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

2 Alan Paller, "SANS What Works in Security Architecture Summit 2010," Las Vegas, Nevada, May 2010.

This risk disclosure could also help to identify solutions to the root cause of the problem. Companies would demand industry-led innovation with a newfound sense of urgency, in order to eliminate or mitigate the risk 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 would have an increased market-driven requirement to deliver products that perform with higher assurance levels. The research community would also have access to data that would facilitate idea creation and innovative solutions to increase security across the entire architecture.

The increased data that would result from such risk filings could also lead to the growth of an insurance industry to help companies absorb costs if the data shows a minimum standard of due care. Some insurance companies are beginning to offer policies designed to protect businesses should they fall victim to intrusions or other forms of online disaster. However, there is still not enough actuarial data on which to reliably base the premium rates.[3] If companies were required to disclose intrusions and the associated external costs of lost intellectual property or lost productivity, then insurance policies and costs would be more predictable. 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 would provide adequate protection, taking into account risk requirements and business operations. Then, if a corporation had implemented adequate defenses of its networks or information assets, and a breach occurred (e.g., illegal copying and movement of data), it could call upon its insurance plan to supplant the losses. Such action would lead to a discussion of liability, and may in fact reveal the legal underpinnings associated therein.

This proposal may seem dramatic, and industry may appeal based on the unintended consequences of implementing such a rule in this area, arguing 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, illustrated by the Enron case, among others. And why shouldn't the SEC take measures to protect the near-term economic infrastructure and long-term growth for publicly traded companies?

3 David Briody, "Full Coverage: How to Hedge Your Cyber Risk," *Inc.*, April 1, 2007, www.inc.com/magazine/20070401/technology-insurance.html.

"...the President can also turn to the Federal Communications Commission (FCC) to enlist private-sector talent, requiring the core telecommunications providers and ISPs to shoulder more of the burden of protecting our infrastructure."

Turning to the Federal Communications Commission

Concurrent with the SEC option, the President can also turn to the Federal Communications Commission (FCC) to enlist private-sector talent, requiring the core telecommunications providers and ISPs to shoulder more of the burden of protecting our infrastructure. The major telecommunications providers and ISPs collectively have unparalleled visibility into global networks, which enable them with the proper tools to detect cyber intrusions and attacks as they are forming and transiting toward their targets.[4] They even have the ability to tell the consumer if a computer or network has been infected. For example, Comcast is "expanding a pilot program that began in Denver last year, which automatically informs affected customers [by sending them] an e-mail, urging them to visit the company's security page."[5] Customers are receiving alerts, being offered antivirus customer service, and receiving free subscriptions to Norton security software. While this enhanced service is in the nascent stages, these companies also employ sophisticated tools and techniques for countering attacks to their own infrastructure and the networks. So, why doesn't the FCC mandate that this service be provided more generally, to clean up our infrastructure? Doing so could open a dialogue or lead to a 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.[6]

4 U.S. House of Representatives, HR 5136, 111th Congress, National Defense Authorization Act of 2011.

5 Brian Krebs, "Comcast Pushes Bot Alert Program Nationwide," *Krebs on Security,* 4 October 2010, http://krebsonsecurity.com/2010/10/comcast-pushes-bot-alert-program-nationwide/.

6 The Telecommunications Act of 1996, Pub. L, No. 104-104, 110 Stat. 56. The 1996 Telecommunications Act included a "Good Samaritan" provision designed 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]).

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) on its private infrastructure is a priority for national defense. As such, the German Federal Office for Information Security (BSI) has mandated its ISPs to track down infected machines and advise users on how to clean their computers.[7] Similarly, Australia's ISPs have adopted a code of conduct designed to mitigate cyber threats and to inform, educate, and protect their users from cybersecurity risks.[8] The European Parliament and Council of Ministers reached an agreement on pan-European telecommunications reform that will be transposed into national law 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).[9]

> "'...the Internet will not reach its full potential as a medium until users feel more secure than they do today when they go online.' This is why the President needs to turn to the Federal Trade Commission (FTC) to engage the public on cybersecurity."

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 also would focus innovation toward more sophisticated threats, and would establish a baseline of security for the broader infrastructure. Further, the FCC could request that a reporting function be 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.[10] Further, the information base they create would cut across all segments of the private and public sector, indicating where resources should be placed first.

This type of service should be required not only of the "traditional" telecommunications carriers, like AT&T, Verizon, and Sprint, but should also apply to other ISPs who are providing core communications services, like Comcast, Cox Communications, and Time Warner Cable. It should also include Google, Microsoft, and Amazon, because of their Cloud services. The rapid adoption of technology and growing migration of essential services delivered on Internet-based infrastructure demands that the FCC classify broadband and other Internet services as core telecommunications. This is important, because as the communications infrastructure migrates from older to newer technologies, services like energy (Smart Grid) and public safety (voice-over IP), will be carried over a communications network that may or may not be built to the same standards upheld by the traditional voice telephone system. The FCC realizes that it "needs a clear strategy for securing the vital communications networks upon which critical infrastructure and public safety communications rely,"[11] but is that enough? Key in this debate is how to preserve the open Internet while allowing network operators the flexibility and freedom to manage their networks even as they provide security to our core infrastructure. Also central to this debate is whether to hold wireless broadband and wireline carriers to the same standard when growth will be derived by wireless services and technologies in the coming decade.[12]

Whether wireline or wireless, the FCC needs to take a stance to ensure that carriers contribute to the security and resiliency of our communications infrastructure. After all, this is the very service they guarantee will be available 100 percent of the time; 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 illegally copy their intellectual property. It would help the average at-home consumer take action to address a compromised PC on their home network. And it would help the government to gain a better understanding of the malicious activity occurring inside the very networks and infrastructures that are key to the nation's economic growth and security posture.

7 John Leyden, "German ISPs Team Up with Gov Agency to Clean Up Malware," *The Register*, December 9, 2009.

8 Ben Bain, "Australia Taps ISPs to Fight 'Zombies,'" *Federal Computer Week*, June 29, 2010, 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.

9 http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2009:337:SOM:EN:HTML.

10 U.S. House of Representatives, HR 5136, 111th Congress, National Defense Authorization Act of 2011.

11 The U.S. Federal Communications Commission, "Connecting America: The National Broadband Plan," March 16, 2010.

12 Nilay Patel, "Google and Verizon's Net Neutrality Proposal Explained," Engadget, August 9, 2010, www.engadget.com/2010/08/09/google-and-verizons-net-neutrality-proposal-explained/.

Turning to the Federal Trade Commission

As Commerce Secretary Gary Locke recently discussed, "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 smartphones; nearly 20 percent of taxpayers file [their] 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."[13] This is why the President needs to turn to the Federal Trade Commission (FTC) to engage the public on cybersecurity.

Criminal activity targeting 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 by compromising our computers through scams, spam, and malicious software. They adapt to whatever information-security measures are in place so they can continue to rob our bank accounts, steal our credit cards, and assume our identities. The Federal Trade Commission has a broad mandate to protect and 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 realistic steps to guard against reasonably anticipated 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 guard against Internet fraud, secure their computers, and protect their 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 that would require all e-commerce transactions to carry a warning banner or label, informing consumers that they are assuming a risk by conducting e-transactions—that, in fact, their transactions may not be secure, and could lead to compromised credentials. This can be compared to the warning labels found on tobacco and alcohol products, telling consumers they can be hazardous to their health.

> "If the Obama administration truly seeks to make cybersecurity a national priority, it must move from the tactical programs instituted thus far which reinforce the militarization of cyberspace..."

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 would help to raise awareness for every person who executes online 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.[14] This trend is expected to continue, while at the same time, security analysts anticipate that cyber crimes will increase by more than 20 percent on a year-to-year basis. Consumers must be made aware of the risks of e-commerce, and providers have a responsibility to do everything possible 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—including secure encrypted envelopes, digitally signed critical information, and protected serial numbering—and finding ways 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 remain fertile ground for an expanding range of commercial and consumer activity while also doing a better job of informing Americans of the forces that put consumer e-commerce activity at risk.

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

14 U.S. Census Bureau, "Quarterly Retail E–Commerce Sales: 4th Quarter 2008," February 16, 2010.

Summary

If the Obama administration truly seeks to make cybersecurity a national priority, it must move from the tactical programs instituted thus far which reinforce the militarization of cyberspace with the creation of Cyber Command and other identity-management steps articulated in the National Strategy for Trusted Identities in Cyberspace. We need real leadership and bold steps if we are to improve cybersecurity in the United States. While not everyone will embrace this proposed economic triad of regulation, these initiatives would serve as a catalyst for change, and constitute a much-needed "shot-in-the-arm" to raise awareness and boost our national cyber defense immediately. These initiatives would also signal to the international community that the United States is seriously committed to solving this problem.

This administration has few tools left in its arsenal to address these issues during the remaining half of the President's term. It is a bold step to turn to independent regulatory bodies, but this option is the sole prerogative of the President. While there are those who will resist this proposal, it will certainly spark debate and dialogue, which will accelerate a responsible review of the problem. We need to raise national awareness, and quickly. We can no longer afford to have a polite conversation or, worse yet, remain silent. Rather, we need to be moved by the urgency and gravity of the situation to develop an exquisite understanding of what is at stake. Using good old-fashioned American ingenuity, we can work together to create and drive an innovation agenda that will strengthen our information-security posture, perhaps gaining economic strength as we increase our productivity. This proposal, if implemented, will create the demand curve for cybersecurity and reduce the losses being sustained on a daily basis by our companies and citizens.

December 2010

The Atlantic Council's Board of Directors

CHAIRMAN
*Chuck Hagel

CHAIRMAN, INTERNATIONAL ADVISORY BOARD
Brent Scowcroft

PRESIDENT AND CEO
*Frederick Kempe

CHAIRMAN EMERITUS
*Henry E. Catto

VICE CHAIRS
*Richard Edelman
*Brian C. McK. Henderson
*Franklin D. Kramer
*Richard L. Lawson
*Virginia A. Mulberger
*W. DeVier Pierson

TREASURERS
*Ronald M. Freeman
*John D. Macomber

SECRETARY
*Walter B. Slocombe

DIRECTORS
*Robert J. Abernethy
Timothy D. Adams
Carol C. Adelman
Michael A. Almond
Richard L. Armitage
*Michael Ansari
*David D. Aufhauser
Ralph Bahna
Nancy Kassebaum Baker
Donald K. Bandler
Lisa B. Barry
Thomas L. Blair
Susan M. Blaustein
*Julia Chang Bloch
Dan W. Burns
R. Nicholas Burns
*Richard R. Burt
Michael Calvey
Michael P.C. Carns
*Daniel W. Christman
Wesley K. Clark
Curtis M. Coward
John Craddock
*Ralph D. Crosby, Jr.
Thomas M. Culligan
W. Bowman Cutter
Brian D. Dailey
Robert E. Diamond, Jr.
Paula Dobriansky
Markus Dohle
Lacey Neuhaus Dorn
Conrado Dornier
Eric S. Edelman
Thomas J. Edelman
Thomas J. Egan
Stuart E. Eizenstat
Julie Finley
Lawrence P. Fisher, II
Lucy R. Fitch
Barbara Hackman Franklin
*Chas W. Freeman
Carlton W. Fulford
Jacques S. Gansler
*Robert Gelbard
Richard L. Gelfond
*Edmund P. Giambastiani, Jr.
*Sherri W. Goodman
John A. Gordon
C. Boyden Gray
Marc Grossman
Stephen J. Hadley
Ian Hague
Harry Harding
Rita E. Hauser
Annette Heuser
Marten H.A. van Heuven
Mary L. Howell
Benjamin Huberman
*Robert E. Hunter
Robert L. Hutchings
William Inglee
Wolfgang Ischinger
Robert Jeffrey
*A. Elizabeth Jones
George A. Joulwan
Francis J. Kelly
L. Kevin Kelly
Robert M. Kimmitt
*James V. Kimsey
*Roger Kirk
Henry A. Kissinger
Philip Lader
Muslim Lakhani
Robert G. Liberatore
Henrik Liljegren
*Jan M. Lodal
Izzat Majeed
Wendy W. Makins
William E. Mayer
Barry R. McCaffrey
Eric D.K. Melby
Jack N. Merritt
Franklin C. Miller
*Judith A. Miller
Alexander V. Mirtchev
Obie Moore
*George E. Moose
William A. Nitze
Hilda Ochoa-Brillembourg
Philip A. Odeen
Ana Palacio
Torkel L. Patterson
William J. Perry
*Thomas R. Pickering
Andrew Prozes
Arnold L. Punaro
Kirk A. Radke
Joseph W. Ralston
Norman W. Ray
Teresa M. Ressel
Joseph E. Robert, Jr.
Jeffrey A. Rosen
Charles O. Rossotti
Stanley Roth
Michael L. Ryan
Marjorie M. Scardino
William O. Schmieder
John P. Schmitz
Jill A. Schuker
Matthew R. Simmons
Kiron K. Skinner
Richard J.A. Steele
Philip Stephenson
*Paula Stern
John Studzinski
William H. Taft, IV
Peter J. Tanous
Peter Thomas
Paul Twomey
Henry G. Ulrich, III
Enzo Viscusi
Charles F. Wald
Jay Walker
Mark R. Warner
J. Robinson West
John C. Whitehead
David A. Wilson
Maciej Witucki
R. James Woolsey
Dov S. Zakheim
Anthony C. Zinni

HONORARY DIRECTORS
David C. Acheson
Madeleine K. Albright
James A. Baker, III
Harold Brown
Frank C. Carlucci, III
Warren Christopher
Colin L. Powell
Condoleezza Rice
Edward L. Rowny
James R. Schlesinger
George P. Shultz
John Warner
William H. Webster

LIFETIME DIRECTORS
Lucy Wilson Benson
Daniel J. Callahan, III
Kenneth W. Dam
Stanley Ebner
Robert F. Ellsworth
Geraldine S. Kunstadter
James P. McCarthy
Steven Muller
Stanley R. Resor
William Y. Smith
Helmut Sonnenfeldt
Ronald P. Verdicchio
Carl E. Vuono
Togo D. West, Jr.

** members of the Executive Committee*
List as of November 30, 2010

The Atlantic Council of the United States is a non-partisan organization that promotes constructive U.S. leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

1101 15th Street, NW, Washington, DC 20005 (202) 463-7226

www.acus.org