Looking Within to Improve American Cybersecurity

RICHARD F. FORNO

Dr. Richard Forno directs the graduate cybersecurity program at the University of Maryland Baltimore County. His twenty-year career includes helping build the first formal cybersecurity program for the US House of Representatives, serving as the first Chief Security Officer at Network Solutions (the InterNIC), and co-founding the Maryland Cyber Challenge. Richard was one of the early researchers on the subject of "information warfare," and he remains a longtime commentator on the influence of Internet technology upon society. The views expressed in this commentary are his and may not reflect those of his employer.
richard.forno@umbc.edu

If history is any guide, the ongoing attempts in 2012 to improve American cybersecurity through legislation will continue the practice of "admiring the problem" but not provide significant or lasting cybersecurity improvements for the nation. Many of the Internet security concerns first discussed in the mid-1990s still exist today, and the assorted recommendations to remedy them have not changed much, either. What has changed, however, is the importance of the Internet to contemporary society and the increased risks we face as a result of failing to learn from history in our attempts to address the problem of securing America's cyberspace.

For example, in 1996, just before the "Dot-Com Revolution," the Senate Permanent Subcommittee on Investigations conducted a survey of Fortune 1000 companies to explore the then-emerging concerns of Internet security and its importance to the country. In 1997, the "Manhattan Cyber Project" again examined these issues and developed additional recommendations regarding computer and networked systems security. That same year, the report of the Presidential Commission on Critical Infrastructure Protection (PCCIP) echoed those prior findings and offered its own recommendations from a national security perspective. After 9/11, the "National Strategy to Secure Cyberspace" (2003), the President's Information Technology Advisory Committee's cybersecurity report (2005), the "Comprehensive National Cybersecurity Initiative" (2008), the Center for Strategic and International Studies' "Securing Cyberspace for the 44th Presidency" (2008), and the "White House Cybersecurity Policy Review" (2009) all offered similar recommendations, as have numerous other proposals, reports, analyses, task forces, and pundits over the years. Among the most prominent and oft-repeated recommendations include the sharing of cybersecurity information, fostering closer cooperation between government and commercial firms on cybersecurity activities ("public-private partnerships"), funding new cybersecurity research, acknowledging an ever-changing threat landscape, respecting privacy and civil liberties, and developing a public education campaign about cybersecurity.

Unfortunately, technology changes and time passes, but people remain the same. Longtime cybersecurity professionals, myself included, are frustrated that such ideas, when dusted off and reiterated anew, are greeted warmly by Washington policymakers, who typically end up proposing the same solutions again while hoping for a different outcome [1]. (Einstein had a term for this behavior.) Therefore, I offer three new recommendations to counter this trend and, perhaps, lead to meaningful discussions about actually improving American cybersecurity:

First, ***we must realize that many, but certainly not all, of our cybersecurity problems are self-inflicted.*** Although we are enamored by the promise and allure of new computing technologies and services, in our rush to embrace these innovations we often overlook their potential risks to our well-being and ability to remain resilient in the face of adversity. For example, much has been said over the past fifteen years about protecting our national critical infrastructures as they became more interconnected—and as we became more dependent upon them. However, a fundamental problem remains: if, as a nation, we consider something to be a critical national resource whose disruption by a cyber-attack might endanger public safety and security, effectively securing it requires more than a new National Strategy, greater numbers of cybersecurity professionals, or more technological countermeasures. It necessitates spending the time and resources to "raise the bar" at a fundamental technical and operational level to make things more difficult for adversaries or accidents to cause us problems in the first place. Admittedly, this may incur significant upfront costs for critical infrastructure providers to implement but will likely provide them a higher degree of operational resilience, assurance, and cost savings over the long term. The "Build Security In" initiative of the Department of Homeland Security (DHS) represents such an approach toward software development; however, the same concepts also are applicable to new hardware systems and entire technology infrastructures.

Being truthful with ourselves also means that we acknowledge facts that make us uncomfortable regarding our cybersecurity activities and reviewing where we have gone wrong, both in practice and policy. We are barraged constantly with warnings about the dangers (both real and perceived) that Internet-based hackers, terrorists, foreign agents, or criminals pose to the security of our water treatment facilities, power grids, and other national critical infrastructures so vital to society, but we continue to connect them to the public Internet where such adversaries lurk—and then wonder why incidents happen. Evidently, such preventable vulnerabilities exist in our critical infrastructures: a March 2012 White House-sponsored cybersecurity exercise centered around an incident triggered by a hacker gaining access to New York's power grid systems from the public Internet using an email attack known as "phishing" [2, 3]. Yet none of the current legislative initiatives to improve American cybersecurity proposes that these critical systems be removed from the public Internet—an action that would reduce the number of Internet-based attacks on those systems, if not eliminate the danger entirely. In other words, our own behavior makes it easy for costly, and in many cases preventable, cybersecurity problems to occur.

Second, ***our national dialogue about cybersecurity must transcend sensationalism and special interests.*** Apocalyptic and overused terms like "Digital Pearl Harbor" and "Cyber Katrina" or "Cyber 9/11" must be eliminated from the national lexicon in order to allow rationality and facts to form the basis of proactive public discourse about cybersecurity instead of the reactionary fear-based perceptions implied by the use of such phrases. National cybersecurity policy discussions must include experts from across the spectrum of Internet users and the cybersecurity community instead of drawing on the same people representing the same organizations who recite the same talking points as they have over the past fifteen years—including those who stand to profit by providing solutions to persistent and unresolved cybersecurity problems [4], whose unrelated legislative concerns might disrupt normal cybersecurity activities and routine Internet

operations [5], threaten constitutional liberties [6], or override existing legal protections [7, 8].

Information is crucial to establishing a common understanding and for conducting objective analysis of problems. Therefore, since many cybersecurity concerns are shared by government, business, and individual users alike, minimizing the amount of cybersecurity information that is classified, instead of increasing the number of people granted access to the allure of secret information (much of which is needlessly made secret to begin with), will assist this process of public understanding and is something that even former CIA and NSA Director Michael Hayden agrees with [9]. An expanded public understanding of our cybersecurity situation can indirectly, if not also more objectively, inform national lawmakers about the current state of cybersecurity when deliberating far-reaching national policies related to it. These simple actions will help ensure that cybersecurity policy discussions are based on the professional knowledge of those most closely working in the field and not exclusively on apocalyptic speculation, special-interest posturing, or information that cannot be analyzed or disputed independently and publicly.

Finally, and perhaps most important, ***there must be meaningful accountability for cybersecurity.*** Inculcating and sustaining a national and deep-seated commitment to cybersecurity success has become marginalized by the all-too-human tendency to cut corners for the sake of convenience. Although many of America's cybersecurity problems are self-inflicted, there are few real consequences faced by those responsible beyond short-term financial costs and adverse publicity. Absent meaningful consequences for cybersecurity failures, there is little incentive to overcome the inertia of the problematic status quo.

In terms of accountability, commercial and government organizations would not integrate emerging technologies [10] into their computing environments without first considering the risks and their ability to function should those resources become denied, disrupted, or degraded through intentional or unintentional incidents. This commits them either to forgo such innovations or spend the requisite resources to ensure that the security and availability of critical infrastructures and citizen data over the long term are not sacrificed in the name of enticing cost savings or operator convenience in the near term. Thus, "accountability" need not be externally applied but can emerge through voluntary internal process improvements—which may or may not involve new expenditures or dramatic changes to daily operations. However, when likely preventable cybersecurity incidents do occur, meaningful external accountability and consequences must be brought to bear upon organizations failing to implement effective cybersecurity practices that would have prevented the incident [11]. Instead, new legislative proposals purporting to improve cybersecurity offer broad indemnification to companies, which allows them to escape responsibility for their actions—or lack thereof—when cybersecurity problems occur [12]. Accordingly, implementing accountability for cybersecurity must also extend to policymakers and regulators for their roles in developing the laws and oversight mechanisms that create or perpetuate such problems, and for creating bureaucratic situations that preclude effective, long-term national leadership on cybersecurity matters.

New laws alone will not solve America's cybersecurity problems. Successfully managing America's cyber risks depends on our ability to be honest with ourselves and having the courage to act from a position of fact and objective, rational knowl-

edge while accepting responsibility for our actions. Only then will we be able to achieve greater effectiveness and long-term sustainability in our national cybersecurity posture, practices, and policies. To do otherwise will demonstrate that we have not learned from history and will perpetuate the problematic situation witnessed today.

References

[1] D. McCullagh, "A Cybersecurity Quiz: Can You Tell Obama from Bush?" *CNET*, May 29, 2009: http://news.cnet.com/8301-13578_3-10252263-38.html.

[2] M. Masnick, "If Phishing Email Can Kill NY Power Grid, Lack of Cybersecurity Legislation Is Not the Problem," *Techdirt*, March 12, 2012: http://www.techdirt.com/articles/20120309/16470618060/if-phishing-email-can-kill-ny-power-grid-lack-cybersecurity-legislation-is-not-problem.shtml.

[3] J. Martinez, "White House Tries Cyber Scare Demonstration to Spur Senate," *Politico*, March 8, 2012: http://dyn.politico.com/printstory.cfm?uuid=BCEC37C2-ABCD-4973-9858-569B77D9EFA5.

[4] J. Brito and T. Watkins, "Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy," *Harvard Law School National Security Journal*, 3(1). Accessed on 15 June 2012 at http://harvardnsj.org/wp-content/uploads/2012/01/Vol.-3_Brito_Watkins1.pdf.

[5] T. Daly, "SOPA: Why Do We Have to Break the DNS?" *Dyn*, December 12, 2011: http://dyn.com/sopa-breaking-dns-parasite-stop-online-piracy/.

[6] B. Ritholtz, "SOPA, PIPA, ACTA . . . What's Next?" *The Big Picture*, January 31, 2012: http://www.ritholtz.com/blog/2012/01/sopa-pipa-acta-%E2%80%A6-what%E2%80%99s-next/.

[7] R. Cringley, "CISPA: Big Brother's Best Friend Forever," *Infoworld*, April 27, 2012: http://www.infoworld.com/print/191952.

[8] D. McCullagh, "How CISPA Would Affect You (faq)," *CNET*, April 27, 2012: http://news.cnet.com/8301-31921_3-57422693-281/how-cispa-would-affect-you-faq/.

[9] K. Poulsen, "Former NSA, CIA Chief: Declassify Cyber Vulnerabilities," *Wired*, March 14, 2012: http://www.wired.com/threatlevel/2011/03/hayden-cyber/.

[10] For example, when examining the benefits of cloud computing services, prospective customers seem concerned with cost savings and how it may "empower" them in new and exciting ways, but overlook what may happen if that cloud (and the data, applications, and services within it) becomes unreachable by users who now are totally dependent on it.

[11] Data loss or privacy incidents resulting from the theft of unencrypted corporate or government laptops are easily preventable using any number of accepted technical and procedural best practices. Failing to implement appropriate data safeguards in such cases should result in meaningful—and motivating—consequences both for the organization and for the employee(s) involved.

[12] L. Beadon, "New Draft of CISPA Announced: Some Progress, Still Big Problems," *Techdirt*, April 13, 2012: http://www.techdirt.com/articles/20120413/15420218488/new-draft-cispa-announced-some-progress-still-big-problems.shtml.