Journal of Strategic Security

Volume 8
Number 4 *Volume 8, No. 4: Winter 2015*

Article 4

Best Practices for Operating Government-Industry Partnerships in Cyber Security

Larry Clinton
Internet Security Alliance, lclinton@isalliance.org

pp. 53-68

Best Practices for Operating Government-Industry Partnerships in Cyber Security

Author Biography

Larry Clinton is President of the Internet Security Alliance (ISA). He is the primary author of ISAs "Cyber Social Contract" which articulates a market-based approach to securing cyber space. In 2011, the House leadership GOP Task Force on cyber security embraced this approach. In 2012, President Obama abandoned his previous regulatory-based approach in favor of the ISA Social Contract model. The ISA document is the first and most often referenced source in the President's, "The Cyber Space Policy Review." He is also the primary author of the Cyber Security Handbook for corporate boards published by the National Association of Corporate Directors (NACD) in 2014. In 2015, Mr. Clinton was named one of the nation's 100 most influential persons in the field of corporate governance by NACD. He has published widely on various cyber security topics, testifies regularly before Congress and other government agencies including the NATO Center for Cyber Excellence.

Abstract

Since the publication of the first National Strategy to Secure Cyber Space in 2003 the US federal government has realized that due to the interconnected nature of the Internet, securing the system would require an industry-government partnership. However, defining exactly what that new partnership would look like and how it would operate has been unclear. The ramifications of this ambiguous strategy have been noted elsewhere including the 2011 JSS article "A Relationship on the Brink" which described the dysfunctional state of public private partnerships with respect to cyber security. Subsequently, a joint industry-government study of partnership programs has generated a consensus list of "best practices" for operating such programs successfully. Moreover, subsequent use of these principles seems to confirm their ability to enhance the partnership and hopefully helps ameliorate, to some degree, the growing cyber threat. This article provides a brief history of the evolution of public-private partnerships in cyber security, the joint study to assess them and the 12 best practices generated by that analysis.

Introduction

Shortly after taking office in 2009, President Barak Obama called for a comprehensive review of the nation's approach to combating cyber threats. The President said:

> "The Federal Government cannot succeed in securing cyber space if it works in isolation. The public and private sectors interests are intertwined with a shared responsibility for ensuring a secure, reliable infrastructure upon which businesses and government depend…Only through such partnerships will the United States be able to enhance cyber security and reap the full benefits of the digital revolution."[1]

This article is an attempt to review the nation's approach to combating cyber threats, and how "best practices" for public-private partnerships may help ameliorate—to some degree—growing cyber threats. The first section describes a brief history of the evolution of cyber-focused public-private partnerships, followed by a discussion of case studies in how such partnerships have demonstrated effective results in enhancing cyber security through a robust assessment process. The article concludes with 12 best practices generated by that analysis for more effective management of cyber partnership activities. Ideally, partnerships would continue to evolve to share leadership, appreciate differing perspectives, and develop shared goals and priorities. The digital economy increasingly requires this kind of collaborative environment to continue to flourish, encouraged by the meaningful cyber security accomplishments of public-private partnerships.

A Brief History of the Public-Private Partnership (PPP) for Cyber Security

When the first National Strategy to Secure Cyber Space[2] was written in 2003 the mutually shared nature of the Internet led to the proposition that cyber space would best be secured through a partnership of mutual benefit. It was assumed that industry's natural interest would lead it to develop adequate technologies and practices to secure the expanding cyber systems.

---

[1] Executive Office of the President, "Cyberspace Policy Review; Assuring a Trusted and Resilient Information and Communications Infrastructure," *White House.gov*, 2009, available at: *https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.*

[2] President's Critical Infrastructure Protection Board, *The National Strategy to Secure Cyberspace* (Washington, D.C.: President's Critical Infrastructure Protection Board, 2002).

Government's role was initially thought to be primarily securing its own systems. With respect to the private sector, government's role was largely confined to education, international coordination and assisting with R&D. Market efficiency was assumed to be sufficient to drive adoption of adequate protective measures.

By the time the first National Infrastructure Protection Plan (NIPP)[3] was written in 2006 and updated in 2013[4] a more sophisticated understanding of digital economics made it apparent that the public and private sectors had "aligned, but not identical, interests" with respect to cyber security. Experience demonstrated that commercial security levels were generally lower than those required for national security and other governmental purposes. The NIPP clarified that a voluntary partnership model that could respond to the quickly changing cyber environment was in the nation's national and homeland security interests. However, for this voluntary model to succeed, government would need to do more than just rely on naked market forces or traditional regulation to prompt the private sector to elevate its security spending to meet national security needs.

The NIPP articulated the notion that, to create a sustainably secure cyber system, government could not rely on the private sector to continually make substantial investments that were commercially uneconomic. Instead, an incentive system similar to those used to achieve social needs in sectors such as agriculture, environment, transportation and others would have to be evolved and applied to the cyber security partnership.

> "The success of the partnership depends on articulating the mutual benefits to government and private sector partners. While articulating the value proposition to the government typically is clear, it is often more difficult to articulate the direct benefits of participation for the private sector…In assessing the value proposition for the private sector….government can encourage industry to go beyond efforts already justified by their corporate business needs to assist in broad scale CI/KR (critical infrastructure/key resource) protection through activities such as…supporting incentives for companies to voluntarily adopt widely accepted security practices."[5]

---

[3] Department of Homeland Security, *National Infrastructure Protection Plan: 2006* (Washington, D.C.: Department of Homeland Security, 2006).
[4] Department of Homeland Security, *National Infrastructure Protection Plan: 2013* (Washington, D.C.: Department of Homeland Security, 2013)
[5] Ibid., p. 15.

http://scholarcommons.usf.edu/jss/vol8/iss4/4
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1456

There were periodic efforts to redefine the partnership model to secure cyber space in such a way as to mimic the traditional government-industry regulatory model. The most prominent of these efforts was legislation, which combined efforts of the Senate Homeland Security Committee and Commerce Committee in 2012. This combined bill, drafted under the auspices of Senate Majority Leader Harry Reid and generally referred to as "Lieberman-Collins bill," would have empowered the Department of Homeland Security to set cyber security mandates for large portions of the private sector and grant DHS compliance authority backed by substantial penalties for non-compliance. It defined this new partnership in the following way:

> "This bill creates a dynamic partnership between government and the private sector in which the private sector is responsible for enhancing security of the nation's most critical infrastructure while the government ensures effective oversight and compliance."[6]

Perhaps not surprisingly, industry found this construction of the partnership somewhat strained.

The idea that the private sector would fund national defense needs, including defending against potential nation-state attacks against critical infrastructure, was both naive and impractical. As Busch and Austen Givens pointed out in one of the few academic analyses of public private partnerships, "Any business executive who suddenly announced he was increasing security spending by 25 percent for the good of the nation would almost certainly be fired."[7]

This is not to say that industry is unwilling to spend on cyber security. In fact, industry spending on cyber security has more than doubled in recent years and is now over $100 billion a year.[8] By comparison, DHS spending on cyber security is just over $1 billion annually and total federal government spending is under $15 billion.[9]

---

[6] Cybersecurity Act of 2012, S. 3414, 112th Cong. (2012).

[7] Nathan E. Busch, and Austen D. Givens, "Public-Private Partnerships in Homeland Security: Opportunities and Challenges," *Homeland Security Affairs* 8: 18 (October 2012), available at: *https://www.hsaj.org/articles/233*.

[8] Ponemon Institute, "Cyber Security Incident Response: Are We as Prepared as We Think?" *Lancope*, (January 2014), available at *http://www.lancope.com/files/documents/Industry-Reports/Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf/*

[9] *National Infrastructure Protection Plan: 2006*.

In addition to the financial issues that undermine the attempt to define a traditional regulatory approach as a partnership, there were numerous other reasons why the regulatory approach to cyber security was ill founded, which have been detailed elsewhere.[10] These include the generally unfounded assumption that the primary reason for successful cyber-attacks is corporate malfeasance by under-funding security as opposed to the inherent weakness in the technology and the sophistication of the attackers. There has also been notable lack of success for the regulatory approaches that have been tried in this area, such as HIPPA (health care) and Gramm-Leech-Bliley (financial services), and the enormous negative economic impact that imposing a government-centric regulatory regime would have on goals as desirable as security such as innovation, economic growth, and job creation.[11] As a result of all these problems and despite holding a strong majority in the Senate, the Lieberman-Collins bill couldn't get enough support to even get to the floor.

Following the collapse of the regulatory effort to impose cyber security mandates on critical infrastructure, President Obama issued Executive Order 13636 in February of 2013, which was accompanied by PDD-25. Both documents embraced the voluntary model of industry-government partnership for cyber security and more fully defined several of the elements that would be necessary for it to succeed. The President's Executive Order largely followed the "Cyber Security Social Contract" paradigm that had been proposed by a coalition of industry and privacy groups.[12]

This renewed and more fully articulated partnership model called for industry to work collectively with government through the National Institute of Standards and Technology (NIST) to identify industry based standards and practices worthy of voluntary adoption by critical infrastructure owners and operators. This framework was to be voluntary, scalable, cost effective, and prioritized. The Administration pledged not to seek additional regulatory powers for cyber security and to promote voluntary adoption of the targeted standards and practices through the deployment of market incentives.[13]

In a rare case of bipartisanship, the Social Contract model contract was also embraced by the House GOP Task Force on cyber security that had been

[10] Larry Clinton, "A Relationship on the Rocks: Industry-Government Partnership for Cyber Defense," *Journal of Strategic Security* 4: 2 (2011): 97-112.
[11] Ibid.
[12] Internet Security Alliance, "Improving our Nation's Cybersecurity through the Public-Private Partnership," White Paper, March 8, 2001.
[13] Executive order 13636; Section 7(d)

http://scholarcommons.usf.edu/jss/vol8/iss4/4
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1456

appointed by Speaker of the House John Boehner.[14] By 2015 there had been such a consensus developed that cyber security would best be addressed through a voluntary industry-government partnership process that independent assessors were reporting that it was difficult to find anyone in the nation's Capital who disagreed with the wisdom of the voluntary partnership model.[15]

How to Make Public-Private Partnerships for Cyber Security Work: Case Studies

Realizing that frustration with the partnership model was building in 2011, the IT Sector Coordinating Council (IT SCC) wrote to DHS Under Secretary for critical infrastructure, Rand Beers, and requested that DHS join with the IT SCC in a process to develop a set of collaborative guidelines for operating effective partnerships for cyber security. Working together, the Government Coordinating Council (IT GCC) for IT and the industry sector coordinating council (IT SCC) devised a three-step program using an adaption of critical incident methodology.

First, leaders from the SCC and GCC would select a sample of six programs that had sought to use the partnership as spelled out in the NIPP. Second, since it was understood that government and industry could look at the same program and come to different conclusions as to its effectiveness, the GCC and SCC were asked to independently analyze the programs by accessing planning documents and interviewing key participants. The goals of the interviews were to assess the participant's judgment as to whether the programs were successful or unsuccessful in meeting their goals, and to identify characteristics of the programs that would explain why the programs were labeled as successful or unsuccessful. Finally, the independent GCC and SCC leadership teams jointly analyzed all the results from step two and attempted to identify common elements that were used in successful and unsuccessful programs. Both government and industry independently agreed which programs fit into the successful and less successful categories and were able to identify a dozen "best practices" that were found to have been commonly used in the successful projects and not in the less successful ones. The results of the study were presented at the annual 2012 IT/Comms Government-Industry "Quad" conference in 2012. A summary of this analysis

[14] Office of U.S. Representative Thornberry, "Recommendation of the House Republican Cyber Security Task Force," October 2011, available at: *http://thornberry.house.gov/uploadedfiles/cstf_final_recommendations.pdf*.
[15] Jarno Limnell, "Cybersecurity Is a Team Sport," *Politico,* May 15, 2015, available at: *http://www.politico.eu/article/cybersecurity-is-a-team-sport/*.

and its results follows.[16]

A Partnership Success Story: The 2006 National Infrastructure Protection Plan (NIPP)

Development of the 2006 NIPP was the result of a collaborative process that reflected multiple rounds of stakeholder review and comment during which the Department received thousands of individual comments. The private sector was given the opportunity to participate in the NIPP 2006 drafting process and reported that DHS made a genuine effort to include them in its development. The final 2006 NIPP recognized that partnership is the appropriate model for coordination between industry and DHS. In addition, existing cross-sector organizations or their predecessors (like the Partnership for Critical Infrastructure Security) participated and provided a valuable cross sector viewpoint to the 2006 NIPP. Both the government and industry leadership teams agreed that the process used to create the 2006 NIPP was an example of partnership success.

What Was Successful and Unsuccessful in This Effort

Early involvement by industry in the 2006 NIPP development was judged to be a key to a successful product. The opportunity for industry to provide inputs as the document was being developed was judged by both DHS and the IT SCC as fundamental to the success of the final document. Among the characteristics praised by both industry and the government were:

- Co-drafting: Reflection of private sector comments in the final language demonstrated that DHS respected and was listening to its partner.
- Personal commitment by DHS: DHS Assistant Secretary for Infrastructure Protection Robert Stephan owned the NIPP 2006 process and was committed to partnership with all the stakeholders – including the critical infrastructures—in drafting it. He frequently showed his engagement and leadership by engaging directly in draft language related discussions with stakeholder groups in calls or in person.
- Personal commitment by industry: The leaders of industry's Sector Coordinating Councils (SCCs) and Information Sharing and analysis Centers (ISACs) and other bodies were equally engaged.

[16] Information Technology Sector Coordinating Committee, "Best Practices for Partnership," *Internet Security Alliance*, 2012.

http://scholarcommons.usf.edu/jss/vol8/iss4/4
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1456

A Partnership Success Story: The IT Sector Baseline Risk Assessment

The IT Sector Baseline Risk Assessment was developed as part of the Sector's implementation of the Sector Specific Plan (IT SSP). The Risk Assessment departed from the traditional physical risk assessments, which focused on identifying critical assets and instead identified six "Critical Functions" that the IT Sector provides. The goal of the assessment was to identify high consequence/high likelihood events to prioritize risk mitigation resources and efforts.

Over 70 subject matter experts from industry and government participated in the development of the IT Sector Baseline Risk Assessment. The IT SCC and IT GCC each appointed a co-chair to the committee that developed the Risk Assessment, thereby providing joint authority and accountability. The co-chairs met regularly to develop and map timelines, plan future meetings, track ongoing initiatives, and resolve any conflicts. The committee of industry and government subject matter experts met two to four times a month to develop the risk assessment methodology. Both industry and government judged this program a successful partnership.

What was Successful and Unsuccessful in this Effort

Among the characteristics praised by both industry and the government were:

- Having industry and government co-chairs ensured joint accountability and authority, with defined roles and responsibilities for each co-chair.
- Committee decisions were made on a consensus basis, with extensive efforts to accommodate all reasonable considerations.
  Support staff captured action items and impartially drafted meeting materials based on committee discussions, as opposed to any pre-determined or hidden agenda.

A Partnership Success Story: The Cyber Space Policy Review

Shortly after taking office, President Obama assigned staff of the National Security Council to conduct an intensive review of our nation's cyber readiness—both public and private. This process led to the publication of the Administration's signature document on cyber security—The Cyber Space Policy Review (CSPR). The CSPR was a "clean slate review" assessing all US policies and structures for cyber security. The review team of government

cyber security experts actively engaged and received input from a broad cross-section of industry, academia, the civil liberties and privacy communities, state governments, international partners and the legislative and Executive branches. The review team systematically reached out to the specifically designated elements of the public private partnership as identified in the NIPP, such as the SCCs and the ISACs. The process was multi-faceted including both public and private meetings of substantive nature and an active effort was made to solicit written input from stakeholders. Both industry and government assessed this program as an example of a successful partnership.

What was Successful and Unsuccessful in the Effort

Among the characteristics praised by both industry and the government were:

- Starting with a "clean slate". The review team did not betray a bias toward a particular ideology or approach but rather sought to openly solicit perspectives of all elements of the partnership and then integrate them into a coherent volume.
- Broad stakeholder involvement. The review team of government cyber security experts actively engaged and received input from a broad cross section of stakeholders. The drafters clearly had listened to the various inputs as is evidenced in the numerous quotations from these inputs cited in the Review.
- Utilizing the NIPP. The review team systematically reached out to the specifically designated elements of the public private-partnership as identified in the NIPP.
- Input. An active effort was made to solicit written input from stakeholders.
- Early engagement with the private sector.

A Less Successful Partnership Effort: Industry Integration into the National Infrastructure Coordination Center

Building a joint industry-government cyber operations center had been a longstanding goal of both industry and government. Although this initiative was not technically a joint SCC and GCC initiative, it did involve open operational collaboration and engagement between industry and government. Specific NSTAC members created a Concept of Operations (Con Ops) for the joint operations center and it was subjected to a pilot program. Members of the pilot program agreed to the Con Ops, thereby providing binding partners

http://scholarcommons.usf.edu/jss/vol8/iss4/4
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1456

to the same program rules and operations. A common portal was used so that participating organizations could share information and see what others submitted and "Cross Sector Analysts" were responsible for doing additional correlation and analysis. Both industry and government assessed this program as an example of a less successful partnership.

What was Unsuccessful in this Effort

While DHS used elements of the above program to attempt to build an integrated capability, the program was not developed in collaboration with industry. As a result, analysts from both the IT SCC and the GCC identified various shortcomings with this program. For example:

- There was no common governing document or framework for the program.
- Participants were not told who else was participating in the program, so they did not know who else was receiving the information they shared.
- There was no clarity or transparency on the criteria used to determine who qualified for this program.
- Instead of building situational awareness among participating organizations by providing access to the shared information on a common portal, only DHS analysts had access to the information shared by program participants.

A Less Successful Partnership Effort: Information Technology Supply Chain Risk Management Collaboration

Both industry and government had agreed to develop cohesive policy to manage cyber security supply chain risk. Unfortunately, the private sector felt blocked in its efforts to collaborate due to the lack of information sharing regarding DHS efforts. The private sector felt the lack of information sharing was undermining the public-private partnership as well as fueling the proliferation of multiple, uncoordinated efforts to address supply chain risk management issues within the U.S. Government. Both industry and government assessed this program as an example of a less successful partnership.

What was Unsuccessful in this Effort

Overall, the general lack of communication by government to industry was mutually judged to be unproductive and had the potential to breed

misinformation, which exacerbated the challenge of building an effective public-private effort. Specifically it was found that:

- DHS did not share details or specific supply chain risk management assessment or evaluation criteria and other practices and policies that they were considering applying to the private sector.
- DHS declined to engage in a substantive discussion regarding current IT supply chain risk management practices and standards or potential policies and regulations, when requested by the private sector.

A Less Successful Effort: Blueprint for a Secure Cyber Future—The Cyber Security Strategy for the Homeland Security Enterprise Program and Fundamentally Altering the Public-Private Partnership

Although the National Infrastructure Protection Plan and the Cyber Space Policy Review both articulated the need for a voluntary public-private partnership, and government officials publically had testified pledging their support for this effort, DHS launched a series of policy programs inconsistent with this direction.

One prominent example was the so-called "Blueprint" and "Enterprise" programs. The policy papers accompanying these programs argued that the voluntary partnership was not working and that there was a need to alter the voluntary public-private partnership and fundamentally change it into a traditional regulatory model. At no point did DHS or any other federal agency engage the partnership model to explain why this change in philosophy had been reached, or what the evidence was that problems related to cyber security issues were the result of market failures. When the existence of these efforts came to light, elements of the partnership were asked for only limited input and advised they would be engaged only at the implementation stages. Both industry and government assessed this program as an example of a less successful partnership.

What was Unsuccessful in this Effort

Many in the private sector found it disingenuous for elements at DHS to advocate for a fundamentally different structure of the partnership model (switching from voluntary to a government mandate system) without ever engaging the partnership model to discuss the reasons for this dramatic change. The lack of trust these efforts engendered was magnified as DHS

http://scholarcommons.usf.edu/jss/vol8/iss4/4
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1456

publically espoused the benefits of the partnership model. The papers created ill will and undermined the ability for the partnership to function in the national interest. As a result, the Partnership for Critical Infrastructure Security (PCIS), which represents all critical industry sectors, formally protested these non-partnership activities to Secretary Napolitano and noted that the mistrust these programs engendered truncated partnership programs as DHS eventually acknowledged. Specific items cited as problematic in the "Blueprint" effort were:

- While it is clearly stated in the NIPP that economics are a central issue in developing a sustainable cyber security partnership with the private sector, DHS never produced any economic analysis. As a result the "blueprint for the cyber eco-system" failed to even consider one of the most central elements of that econ-system. Analyses from both the government and industry agreed in retrospect that this critical omission would not have occurred if a more inclusive process had been used.

Cyberstorm and National Level Exercise

The Cyber Storm Exercise series and the National Level Exercise series have been opportunities to leverage the partnership to help manage risks. National Level Exercises: NLE2012 was the first tier 1 exercise on cyber, and was an opportunity to leverage the partnership to enhance prevention, detection, and operational and policy response. Many of the lessons learned through the Cyber Storm series however were not leveraged for NLE2012. The exercise series has received mixed reviews with some notable successes and sustained criticism for the lack of follow through from the exercises.

What was Unsuccessful in this Effort

Analysts reported both successful and unsuccessful elements of the series. Among the successful items were:

Early Strategic Engagement

- Integrating participating communities in a joint coordinated planning process.
- Enabling participating organizations and sectors to identify objectives, and ultimately harmonize those so that ALL participants gained value, and exercise play was appropriately synchronized and coordinated via a core scenario.
- Establishing a National Private Sector Working Group to engage the

participation and expertise of a wide range of private sector stakeholders.

Room for Improvement

- While NLE 2012 raised awareness about cyber risks to a broader community and examined intergovernmental coordination to some degree, the insights could have been greater for all participants if the partnership had been more fully leveraged.
- The findings and recommendations in NLE 2012 were notably similar to many recommendations from previous exercises, including the Cyber Storm Exercise series. Marginal improvements occurred, but meaningful and substantial progress to coordinate and enhance the collective cyber security response capability between government and industry was not made.

Best Practices Generated by the Joint DHS Private Sector Case Studies

Based on the joint government-industry analysis of the six partnership projects summarized above, a set of a dozen best practices that consistently generated successful partnership programs on both a substantive and operational maintenance level were agreed to. Subsequently the PCIS, which is the body designated in the NIPP to represent all the critical industry sectors, endorsed the best practices and has urged DHS to officially embrace them as well. As of this writing DHS has proposed a Memo of Understanding to the PCIS that will embrace these principles for operating future partnership programs. These best practices are:

- Senior level commitment to the partnership process communicated to staff & upper echelons.
- Involvement at the priority/goal and objective phases of projects, not just implementation.
- Use of the process identified in the NIPP for involving industry.
- Reaching out to stakeholders early on, ideally at the "blank page" stage.
- Continuous and regular interaction between government and industry stakeholders.
- Providing adequate time for stakeholder review (equivalent to government review).
- Establishing co-leadership of programs

http://scholarcommons.usf.edu/jss/vol8/iss4/4
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1456

- Consensus partnership decision making.
- Communicating genuine interest in stakeholder input e.g. via co-drafting.
- Adequate engagement from federal agencies beyond DHS
- Government follow through on partnership related decisions
- Adequate and competent support services

Following Best Practices in Regulated and Unregulated Industries: More Success Stories

The NIST Cyber Security Framework

President Obama's Executive Order 13636 on Cyber security instructed NIST to launch a collaborative process with industry designed to develop a "framework" for critical infrastructure cyber security. Rather than impose the subsequent framework by seeking additional regulatory authority, as it had done previously through the Lieberman-Collins bill, the Administration pledged to retain a voluntary approach supplemented by the deployment of a set of market incentives.

This NIST process embodied virtually every one of the best practices identified in the IT Sector- DHS partnership study. The President himself launched the process via an Executive Order and senior officials regularly reemphasized commitment to the process. NIST made every effort to not only involve industry but also make the framework an "industry framework not a government framework." This included an extensive process of six national workshops across the country that brought in hundreds of stakeholders. This process was complemented by an extensive series of private meetings with interested stakeholders. NIST regularly updated drafts of the Framework with adequate time for industry review and comment and embraced comments and made substantial and clearly evident changes as the process matured. NIST also did not display the sometimes-pernicious tendency of government agencies to claim "ownership" of the process. Perhaps, in part due to the clear direction directly from the President, NIST comfortably folded in adequate engagement from other government agencies.

Although at this writing the final Framework has only been out for just two years, the feedback has been nearly unanimous in praising the process. Michael Daniel, White House special assistant to the president and cyber security coordinator, has called industry's response to the framework "phenomenal." A second White House official, Ari Schwartz, senior director

for cyber security, added that business support for the framework has "exceeded expectations." Such recognition is constructive and helps keep the private sector engaged in using the framework and promoting it with business partners.[17]

From the industry side, the U.S. Chamber of Commerce—which had vehemently opposed the Obama Administration's earlier efforts on cyber security—now echoed the Administration's assessment of the NIST process:

> "The Chamber believes that the release of the Framework for Improving Critical Infrastructure Cyber security has been a remarkable success. The Chamber, sector-based coordinating councils and associations, companies, and other private and public entities collaborated closely with NIST in developing the framework since the first workshop was held in April 2013. Critical infrastructure sectors are keenly aware of and supportive of the framework."[18]

The financial services industry, one of the sectors most targeted and most severely affected by cyber- attacks, also expressed strong support for the NIST process.

> "Regarding the Framework development process, it was a success due in large part to its transparency and because it sought to harmonize various views into a cohesive whole. We applaud that NIST's process for developing the Framework engaged these other sectors during the Framework's drafting. NIST's successful approach at inclusion of so many essential parties is reflected in how broadly embraced the Framework has become across so many sectors."[19]

However, a process that generates a positive effect is inadequate if the larger public policy goals are not met. Here again, the NIST process seems to be generating commitment and advancement to improved cyber security:

> "With respect to the Framework, its true value is that it synthesizes a

---

[17] Steven Chabinsky, "What is the Most Influential Cyber Security Team?" *Security Magazine*, September 1, 2013, available at: *http://www.securitymagazine.com/articles/84677-what-is-the-most-influential-cyber-security-team*.
[18] U.S. Chamber of Commerice, Comments on the NIST Request for Information on the Cyber Framework, October 10, 2014, available at: *http://csrc.nist.gov/cyberframework/rfi_comment_october_2014/20141010_uscc_eggers_rev1.pdf*.
[19] Ibid.

http://scholarcommons.usf.edu/jss/vol8/iss4/4
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1456

process for cyber risk management that is accessible from the boardroom to the operations floor, across not only individual enterprises but also entire sectors. It relies on international standards and is consistent with the regulatory requirements that have been in place for our sector for more than a decade. It is a 'Rosetta Stone' in that it provides a common lexicon for categorizing and managing cyber risks across sectors and enterprises for various unifying risk management jargons and creates a common understanding around various risk management terms, methodologies, ideas and language.

As a result, we have heard from member financial institutions that in terms of internal enterprise usage, Chief Information Security Officers (CISOs) are using the Framework to communicate ideas and achieve "buy-in" for various cyber security initiatives. Externally, firms are beginning to use it to communicate expectations and requirements to vendors."[20]

CSRIC Working Group 4 (FCC and Communications Sector)

The U.S. Department of Commerce has no regulatory authority and hence its sub-division, NIST, might be expected not to utilize a more traditional regulatory model when seeking to promote improved cyber security behavior in the private sector. By contrast, many elements of the telecommunications sector come from a strong and varied regulatory history. Hence, when the Federal Communications Commission (FCC) undertook the task of engaging the industries under its authority to promote improved cyber security practices it might have been expected that they would resort to a legacy model of federal regulations supplemented by adapting historic state and local authorities. However FCC Chairman Tom Wheeler chose instead to call for a "new paradigm" to address the unique challenges of digital technology and asked industry and Commission staff to utilize the Communications Security, Reliability and Interoperability Council (CSRIC Working Group 4) process to find a new way to implement the NIST Framework within the communications industry.

CSRIC Working Group 4 launched a 6-month process to operationalize the "new paradigm" sought by Chairman Wheeler. The process embraced virtually all of the previously identified best practices. And much like the NIST process, the reviews from both government and industry have been starkly positive.

In a featured speech at the 2015 RSA Security Conference, FCC Chairman Wheeler said Working Group 4:

[20] Ibid.

> "...developed a range of activities intended to provide transparent assurances to the FCC, to DHS, to industry, and to consumers. These visible assurances should provide confidence that companies throughout the sector are actually taking effective steps to manage cyber risk... I believe that CSRIC's assurance model will provide much-needed accountability foCSr network security, while avoiding top-down prescriptive regulation of industry practices. A cooperative and collaborative approach is the FCC's preferred means of engagement. I have every reason to be confident the industry will live up to its commitments and deliver meaningful action."[21]

Conclusion

Cyber security is one of the areas of public policy where substantial consensus has emerged. There is broad agreement that the security problem is severe and growing and that the traditional regulatory model does not fit well with unique characteristics of the Internet and the conscious and sustained attacks on it. Instead, a novel, voluntary, and economically sustainable partnership between industry and government needs to evolve. Early efforts at partnership met with inconsistent success.

More recently, however, industry and government have collaborated and identified a set of practical guidelines or "best practices" for managing cyber partnership activities. This more sophisticated notion of partnership departs from having critical functions decided unilaterally by government, with industry's role confined to comment, implementation, or compliance. Instead, the new partnership model requires, among other things, that the partners share leadership, appreciate each other's differing perspectives, and develop partnership priorities, goals, and objectives together.

Notwithstanding the mounting evidence that these partnerships, properly managed, are generating success in an extremely challenging arena, government agencies may be reluctant to depart from the traditional regulatory model for a model that requires more time and collaboration on the front end, and less traditional enforcement on the back end. However, the digital economy of the 21st century may demand an evolution away from the legacy independent regulatory model developed in the 19th century. When utilized, this approach has, at least initially, driven meaningful cyber security accomplishments.

---

[21] Tom Wheeler, FCC Chairman, Prepared Remarks for RSA Conference, April 21, 2015 in San Francisco, CA.

http://scholarcommons.usf.edu/jss/vol8/iss4/4
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1456