Social Contract 2.0:
A 21st Century Program for Effective Cyber Security

Board of Directors

The views expressed in this publication do not necessarily reflect the views held by any individual member of the ISAlliance Board of Directors nor the companies they are employed by.

Thanks and acknowledgment are given to the organizations that supplied experts to this initiative and for their active and ongoing support of the ISAlliance. Recognition is also due to these companies for their ongoing and generous contributions to the cyber security community. Special acknowledgement is due to Jeffery Ritter and Scott Borg. Without the contributions made by all the individuals listed on this page and the collective expertise shared by their companies, this action guide for developing the second phase of the 21st century cyber security social contract would not have been possible.

Table of Contents

MOVING IN THE RIGHT DIRECTION BY ADDRESSING THE ECONOMICS OF CYBER SECURITY

WHY PRESIDENT OBAMA IS ON THE RIGHT TRACK FOR CYBER SECURITY

'Let me make one thing very clear, we are not going to mandate cyber security standards for the private sector."-----President Barack Obama, May 29, 2009 [1]

The Internet Security Alliance believes that the President is on the right track toward developing a sustainable system of cyber security as outlined in his Cyber Space Policy Review, [2] and, then, as reinforced in his White House speech in May 2009.

The current document will extend the "dialogue" called for in the Cyber Space Policy Review by aligning points of agreement between the Administration's Review and the Cyber Security Social Contract: Recommendations for the Obama Administration, published by the Internet Security Alliance in November 2008. A major focus of agreement between these two texts is the appreciation of the economics of cyber security and the need to properly deploy incentives to generate enhanced security within the private sector to serve the broader national interest.

Rewriting the economic equations currently governing cyber security issues is essential to creating the sustainable and evolving system of security that we will need to protect our nation against the emerging threats we are facing in the 21st century.

A system of regulatory mandates applied to the broad and diverse private sector is unlikely to be effective in generating the substantial improvements in private sector cyber security that the ISA has been calling for since its creation in 2001. In fact, such a system would almost certainly be counter-productive, from both a national economic, as well as a national cyber security perspective.

The regulatory agency model of governance was created during the 19th century to address the hot technology of that day—the railroads. And, while rail travel today is remarkably similar to what it was in the 1800s, the Internet, however, is characterized by nearly daily change.

The process of developing effective regulations is inherently time consuming there is virtually unanimous agreement that any regulations specific enough to assure improved cyber security would become outdated soon after their enactment.

Moreover, the regulatory process is, generally, an open process which amounts to the publicizing the US's defensive positions. In addition, the political process through which regulations are created and modified can result in "compromised down" regulations. This process can lead to minimum prescriptions that fall short of meeting their desired goal. An

[1] Remarks by President Obama on securing our nation's infrastructure, May 29, 2009
[2] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure*

example of this sort of regulation is the political campaign finance system, wherein virtually every political candidate in the country can attest to compliance with the national standards, but where no one believes that the standards actually resolve the issues they were designed to address.

While this sort of minimalist approach is acceptable for our political process, we cannot afford a cyber security system that is similarly managed. Moreover, as is documented in the chapter on incentives, attempts to create cyber security regulations have met with limited effectiveness and typically generate increased costs to document compliance while diverting resources from actually enhancing security.

Even more troubling than the low prospect a regulatory mandate model has for success is the fact that such a model would generate seriously negative economic and security consequences.

We live in a world economy. A U.S. mandate system would increase costs uniquely on U.S. companies, making them less competitive at the very time that world competition is most daunting. We've seen this first hand with the Sarbanes Oxley Act of 2002 (SOX), which also had the secondary detriment of reducing the number of private companies that attempt to go public. Moreover, a U.S. mandate system would almost certainly bring government bureaucrats deep into the workings of the business world on an unprecedented technical level, vastly undermining the ability of U.S. firms to innovate and maximize their great creativity.

History shows that, even during the cold war era, nationally centralized industrial systems were slow, inefficient and uncompetitive. Subjecting the U.S. economy to government-determined technology standards would be even more catastrophic in the digital world.

Certainly, investors would not support a system weighed down by government-mandated standards. Requiring that federally-mandated regulatory requirements be built into the cyber systems upon which virtually every sector, and certainly every critical sector, of the economy relies would drive investment dollars overseas in a dramatic fashion. These requirements would result in further economic consequences, including additional job losses, at a time when U.S. unemployment is at its highest point in a generation.

To make matters even worse, among the many jobs that would flee the country would be those for cyber security specialists. Mandated standards would, essentially, create an economic incentive to drive the very personnel we need most (and who are already in short supply) off shore.

The problem is not a lack of will, or effort, or even political courage. The problem is trying to address a 21st century problem, cyber security, with a cold war era governance structure.

These issues are among the reasons why most policy makers and industry leaders applauded President Obama's pledge not to mandate compliance with cyber security standards.

However, the President's statement does beg the question: if the government is not going to provide regulatory mandates, what is the government going to do to encourage improved cyber security?

THE ISA CYBER SECURITY SOCIAL CONTRACT

Shortly after the new President and Congress were elected, the ISA proposed a specific framework, the Cyber Security Social Contract,[3] to offer a specific path to address the dangerous, evolving, international, and novel problem of creating a sustainable system of cyber security.

There are two key elements to the Cyber Security Social Contract. First is the realization that cyber security is not a purely technical problem. Rather, cyber security is an enterprise-wide risk management problem which must be understood as much for its economic perspectives as for its technical issues.

The second key element is that, at this point, government's primary role ought to be to encourage the investment required to implement the standards, practices, and technologies that have already been shown to be effective in improving cyber security.

The fact is that the Internet is constantly under attack, thousands and thousands of times every day. As a result, the market has already developed multiple methods to assist in the Internet's defense. In addition, multiple research studies have documented the success of the standards, practices, and technologies that the market has generated. Expert testimony, including that from sophisticated government representatives, has confirmed that we know how to address the vast majority of these issues, but that we are just not doing it. The key is implementation.

Among the various sources that document the effectiveness of available measures to improve cyber security is "The Global Information Security Survey,"[4] conducted by PricewaterhouseCoopers. The study found that organizations that followed best practices had zero downtime and zero financial impact from cyber attacks, despite being targeted more often by malicious actors.

An almost identical finding was reported in Verizon's "2008 Data Breach Investigations Report." This study drew on over 500 forensic engagements over a four year period including literally tens of thousands of data points. The study states that, in 87% of cases, investigators were able to conclude that a breach could have been avoided if reasonable security controls had been in place at the time of the incident.[5]

---

[3] Internet Security Alliance, *The Cyber Security Social Contract: Policy Recommendations for the Obama Administration and the 111th Congress*

[4] *Is Cyber Security Improving in the Business World, Why? or Why Not?*, Presentation by John Hunt, Principle PricewaterhouseCoopers, on the results of the 2009 Global Information Security Survey. University of Maryland October 28, 2009

[5] Verizon Business Risk Team, *2008 Data Breach Investigations Report* at 2-3

In October 2008, Robert Bigman, the CIA's Chief of Information Assurance, told attendees at an Aerospace Industries Alliance meeting[6] that, contrary to popular belief, most cyber attacks were not all that sophisticated. Mr. Bigman estimated that, "you could reject between 80% and 90% of attacks with the use of due diligence." He also added that, "the real problem is implementation."

On November 17, 2009, Richard Schaffer of the National Security Agency made a very similar assessment in sworn testimony before the Senate Judiciary Committee, in which he asserted that 80% of cyber attacks were preventable using existing standards/practices and technologies.[7]

As detailed more fully in the Information Sharing Chapter of this document, stimulating greater implementation of basic best practices for security would "force intruders into greater costs and complexity" to be successful. Today, it's like walking through a neighborhood to check for unlocked doors; many people can do that. If all of the doors are locked, though, attackers would need to know how to pick locks in order to gain access. A smaller number of attackers have this knowledge, and they would have to execute a more determined attack that takes longer and is more easily identified, both during, and after an attack.

The purpose of this document is not only to continue the dialogue between ISA and its government partners, but also to offer concrete suggestions on a variety of critical cyber security issues in order to assist in the implementation of solutions in all areas where there is already conceptual agreement.

The Cyber Security Social Contract is based on the successful partnership that was created between government and industry to address a similar technology infrastructure development issue in the early 20th century - the need to create universal utility service.

In the early part of the last century, government recognized that there were substantial public safety and economic benefits in universal telephone/power service. To assure that this public need was met, government provided substantial market incentives, essentially in the form of a guaranteed rate of return for private investors who were willing to make the necessary infrastructure investment. The result was that the US became the world model for the provision of what became known as public utility service, thereby benefiting consumers with state of the art services while simultaneously, generating trillions of dollars of economic activity for the nation.

There exists a similar situation today. Just as our nation needed universal utility services a century ago, our nation needs universal cyber security now. In the cyber world, security cannot be guaranteed in isolation. One entity's security is dependent upon the security of all of the entities with which it interacts.

---

[6] Robert Bigman comments to the Aerospace Industries Association Annual Conference on Cyber Security, Washington, DC in October 2008

[7] Written testimony of Richard Schaffer (NSA) to the Senate Committee on Judiciary, Subcommittee on Terrorism and Homeland Security, November 17, 2009

Despite the substantial work and investment that is already being made to address the issue, the investment required for common, that is universal cyber defense, is not justified by the full range of corporate business plans. Therefore, as with utilities, a sustainable and effective system of cyber defense will require the use of market incentives to encourage private corporations to make investments that move beyond their legally-mandated goal of maximizing shareholder value to serve the public interest.

UNDERSTANDING THE ECONOMIC AND FINANCIAL NATURE OF CYBER SECURITY

Until just recently, it was common for information security policy discussions to take place without any reference to economic issues. However, corporate suites are one arena in which these discussions rarely ignore the financial impacts of poor cyber security.

As PricewaterhouseCoopers' 2009 Global Information Security Study[8] documents, economic considerations are actually some of the most important considerations in determining corporate information security spending decisions, and these considerations rate higher than regulatory compliance, company reputation or internal policy compliance, and nearly as high as the number one issue - business continuity/disaster recovery.

Effective and sustainable improvements in our collective cyber security posture will stem from a comprehensive understanding of how to effectively motivate all players across our economic landscape to actively engage in proven best-practices in both their business and individual cyber activities. Fortunately, long-standing research in policy analysis offers both insight and lessons-learned as to what are the optimally effective policy and incentive structures that will achieve the desired improvements in our cyber security posture. An understanding of the proper alignment of incentives and various outcome objectives can provide us with a framework that can be used as the foundation for policy and incentive recommendations for cyber security.

Despite the obvious importance of understanding cyber security economics in the development of public policy, it is little discussed and is often difficult to delineate. Typically, the economics of cyber security are not readily transparent and they are poorly appreciated.

For example, in order to reach their ultimate targets, it is common practice for cyber attackers to capture and use third-party computers. As a result, owners of many compromised computers do not bear responsibilities of an attack since their computers are basically hi-jacked to facilitate a further attack. As such, there are currently no incentives or disincentives in place that would strengthen the defenses of such third-party computers to make these computers resilient to take-over attempts. Moreover, the defense of the ultimate targets of an attack is compromised by the targets' interconnection with these third-party systems.

[8] *Is Cyber Security Improving in the Business World, Why? or Why Not?* Presentation by John Hunt, Principle PricewaterhouseCoopers, on the results of the 2009 Global Information Security Survey. University of Maryland October 28, 2009

For example, the owners of third party computer systems utilized in a cyber attack may not have economic incentives to adequately invest in their computers' defense since they do not suffer the direct economic costs of a cyber attack.

On the other hand, the defensive investments required of the ultimate targets of cyber attacks can be substantially undermined by the weakness of others with whom they are interconnected, thus reducing the return on investment (ROI) generated by their cyber security spending. When defensive investment is compromised by factors beyond an organization's control, the motivation for continued investment is reduced substantially.

There are also substantial internal reasons for failing to recognize the true costs of cyber events. These reasons range from the corporate world's fear of investment loss due to publicity about successful cyber attacks, to consumers' false sense of security due to the belief that personal losses will be fully covered by corporate entities (such as the banks), when, in fact, much of these losses are transferred back to consumers in the form of higher interest rates and consumer fees.

At the federal government level, there seems to be no appreciation of the enormous financial risk that the government itself shoulders from the prospect of a "cyber hurricane." In reality, the federal government is the de-facto "insurer of last resort," and would be faced with footing virtually the entire financial burden of a massive cyber event, much as they did recently for a "financial hurricane." A prudent public policy strategy would be to engage in risk transfer techniques (such as the use of insurance), but there is little evidence that this is occurring on a national level.

Further, as we will discuss later in some detail, corporate structures are built on outdated models wherein the owners of data do not understand themselves to be responsible for the defense of that data. As a result, the financial risk management of cyber events across enterprise settings is not often properly analyzed, nor appreciated.

In addition to organizational problems, the techniques for measuring the success of security programs have not evolved with the new threats. As the sophistication of attacks increases, many organizations do not realize that they have had breaches because the organizations are looking for the wrong indicators. Therefore, the organizations are given a false sense of security wherein it appears that their security posture has improved, and they do not realize the need to spend more on cyber security.

The interaction of these factors may be at the root of the fact that, despite the increasingly publicized dangers of cyber incursions, nearly half (47%) of all of the enterprises studied in the 2009 Global Information Security Study reported that they are actually **reducing or deferring their budgets for information security initiatives**[9].

[9] *Is Cyber Security Improving in the Business World, Why? or Why Not?* Presentation by John Hunt, Principle PricewaterhouseCoopers, on the results of the 2009 Global Information Security Survey. University of Maryland October 28, 2009

Such information security spending decreases are taking place even though many enterprises (42%) acknowledge that the "threats to their information security have increased" and more than half of these enterprises (52%) acknowledge that these cost reductions make adequate security more difficult to achieve[10].

Ultimately, with respect to cyber security economics, the dispiriting realization is that all of the current economic incentives favor cyber attackers:

- Cyber attacks are comparatively cheap and easy to execute.
- The profits that can be generated from cyber attacks are enormous.
- Because of the typically long distance physical proximity, there is very little risk of being caught or suffering retaliation.
- The cyber defensive perimeter is nearly limitless.
- Losses are difficult to assess.
- Defense is costly and often does not generate perceived adequate return on investment.

The ISA Cyber Security Social Contract argues that, much like the utility service model, what will be required is for the public sector to deploy market incentives to motivate private investment for the purposes of protecting the public interest. The government is charged with the responsibility to provide for the common defense. However, in the cyber world, the government cannot do this alone. They will require private sector cooperation and investment. While some of this investment will come from corporations serving their own private security needs, the extent of investment needed to serve the broader public needs, due to some of the unique aspects of cyber economics described above, will be greater than what is justified by private sector business plans.

CONVERGING PUBLIC AND PRIVATE SECTOR APPROACHES TOWARD IMPLEMENTATION OF A SUSTAINABLE MODEL OF CYBER SECURITY

The Obama Administration's policy document was created after a comprehensive review of both public and private sector cyber security. This unprecedented analysis of cyber security was intended, in the report's words, "to conduct a national dialogue" on cyber security.

The ISA believes that the Administration listened well to its view, as well as to the views of many others, as to what ought to be done in regard to cyber security. In fact, the first document cited in the Administration's Cyber Space Policy Review is the ISA's Cyber Security Social Contract. As well, the Executive Summary to the Administration's Review both begins and ends by citing ISA documents and it references more than a dozen other ISA contributions.

The balance of the current publication is designed to identify some of the multiple instances wherein there is, at least on the overall principles, mutual agreement between the ISA's and the Obama Administration's positions on a series of critical policy areas. In each chapter,

[10] *Is Cyber Security Improving in the Business World, Why? or Why Not?* Presentation by John Hunt, Principle PricewaterhouseCoopers, on the results of the 2009 Global Information Security Survey. University of Maryland October 28, 2009

ISA identifies an issue deemed critical by both our organization and the Obama Administration and follows with an extended discussion toward implementing steps to accomplish the common goals.

Before proceeding to the specific policy areas, though, it is important to identify some major overarching points of agreement between ISA and the Administration. Each of these overarching points embraced by the current Administration's position represents a substantial enhancement of previous US government positions, and is in accord with long-stated ISA policy.

First, the current Administration's position correctly assesses the seriousness of cyber security as a national problem that merits a coordinated strategy and response that is managed from the White House itself. During the beginning of the Bush Administration, there was a senior official in the White House who was in charge of addressing cyber security issues, Dick Clarke, but, the position evaporated when he left. Furthermore, it took several years, and considerable industry lobbying and bi-partisan Congressional pressure, for an Assistant Secretary role to be created at the Department of Homeland Security (DHS) and that position remained vacant for one year after its creation.

Despite the need to manage two wars, the worst economic environment in nearly a century, and a series of other domestic priorities, the emphasis that the Administration has placed on cyber security (as evidenced by the production of Cyber Space Policy Review and its recommendations) is encouraging.

Second, notwithstanding the frustrations emanating from the delay in naming a cyber coordinator, the fact that the President himself has delivered a major address on cyber security, and has designed a White House-level office to address the issue in a coordinated and comprehensive fashion, is reflective of the need to address cyber security. Secretary of State Clinton has equated the cyber threat issue with Weapons of Mass Destruction and the issue is generating an estimated annual economic loss upwards of $1 trillion.

Third, the Administration's position is coordinated with the ISA's position in its direct appreciation of the economics of cyber security. While previous Administration documents have at least implicitly acknowledged the economics of cyber security, the Obama Administration places the considerations of economic impact central in its designation of the Administration's chief official on cyber security as a dual-hat position connected to both the National Economic Council and the National Security Council.

Forth, the Administration's position directly advocates the development of market incentives as a key lever in motivating private sector cyber security. The previous Administration's core position was represented in the 2003 National Strategy to Secure Cyber Space (NSSCS), which correctly articulated the need to rely on market forces to generate needed cyber security enhancements.

However, as ISA has argued since the NSSCS was published, the missing link in the previous national strategy was the understanding that modern markets do not spring spontaneously into fully functioning form. When, as in this case, a comprehensive solution is required to serve the public interest, the government needs to use its substantial market powers to motivate action by the private sector that may be independent from, or additional to, the actions required to fulfill a corporation's business plan and its legal obligation to maximize share-holder value (see Appendix A). For the first time, in the Cyber Space Policy Review, the White House has specifically included these critical mechanisms in its tool kit to address US cyber security problems.

Succeeding chapters of this document will discuss a series of distinct issues and will offer extended frameworks to address these issues in a manner consistent with the overarching model described above. In each case, an attempt will be made to apply social contract theory to the issue area and to extend the discussion toward the implementation of collaborative solutions. While all of the frameworks described are already in some degree of implementation, they are, naturally, at varying stages, and each could benefit from further collective work. The issue areas are:

- Creating a new, practical model for information sharing
- Using incentives to develop a market for good security standards and practices
- Creating an enterprise education program to properly structure industry
- Addressing the technical and legal disconnect created by digital systems
- Managing the global IT supply chain
- Addressing the international nature of cyber security issues

CREATING A PUBLIC PRIVATE MODEL TO ENHANCE CYBER SECURITY THROUGH MARKET INCENTIVES

The growing seriousness of the cyber security problem we are currently witnessing demands that new, aggressive, and sustainable methods be implemented to motivate improved cyber security behavior.

The good news is that we actually know a great deal about how to prevent, mitigate and recover from cyber incidents. Although cyber threats continue to evolve and there are a series of serious problems for which we do not have sufficient answers, a great deal of the incidents we are experiencing can be effectively managed simply by putting into effect standards, practices, and technologies that have already been generated by the market. Chapter 1 of this publication cites independent research as well as public and sworn statements from senior CIA and NSA officials all of which agree that between 80%-90% of cyber attacks could be prevented or substantially mitigated by use of currently available methods.

There has also been a growing recognition that the sorts of incentives that are routinely used throughout other areas of our economy, including environment, aviation, agriculture, ground transport, and physical security, may be successfully adapted for use in the cyber security arena. A sample of this consensus is evident from multiple position statements from the ISA, the policy paper on market incentives produced by the Cross Sector Cyber Security Working Group[11] consisting of representatives from both private and public representatives of the 13 officially designated critical sectors, as well as the Obama Administration's Cyber Space Policy Review.

While cyber-security challenges facing our nation are often thought of as new territory, we have the benefit of strong parallels and lessons learned from previous policy strategies applied to problem sets sharing similar characteristics of cyber-security. Long-standing research in policy analysis offers further insight into optimally effective policy structures to achieve changed behavior. Understanding the proper alignment of incentives with various collective objectives provides us with a framework that we can use as the foundation for policy recommendations in the arena of cyber-security.[12] An example of how these policy lessons can be effectively applied to the challenges of cyber-security is seen in Appendix A.

Since we know now, what organizations need to do to enhance their cyber security, and since we have a historic range of incentives that we can apply to motivate improved behavior as well as emerging consensus that deploying such incentives in this field is appropriate, the next step is to weave these factors together into an operational government-industry model that will create a sustainable system of cyber security. This is exactly what the current chapter will attempt to articulate.

[11] Cross Sector Cyber Security Working Group—Incentives Subgroup, *Incentives Recommendations Repor*t, September 21, 2009

[12] Nagel, Stewart S.; Handbook of Public Policy Evaluation; Sage Publications Inc. 2002

Quotations from the ISA Social Contract

"We lack the proper incentives structure to address the information security issues. For too many corporations, simply "fear motivation", whether the result of a regulatory environment or the theoretical potential financial impact of a major cyber event is insufficient to adopt desired loss mitigation and prevention actions. This is especially troublesome given the interdependent nature of the internet where the failure of one institution can rapidly have adverse consequences on other, even better protected, institutions. The mix of positive and negative incentives must be realigned."[13]

"The National Strategy to Secure Cyber Space, while well intentioned in its market orientation, was inadequate in advocating a completely voluntary model. Such a model, while accurate in many corporate situations, does not have the expanse needed to address the broad-based issues in cyber space where the weak link in the chain can break the entire security perimeter. Government must utilize a multi-layered approach that applies regulation where appropriate, such as in consumer protection, with market incentives, which can respond to the fast changing threat sectors faster, more effectively and more broadly than a traditional regulatory model can accommodate."[14]

From the Obama Administration's Cyber Space Policy Review

"Federal policy must address national security requirements, protection of intellectual property, and the availability and continuity of infrastructure, even when it is under attack by sophisticated adversaries. The Federal government also must be careful not to create policy and regulation that inhibits innovation or results in inefficiencies or less security. [15]

"The United States should harness the full benefits of innovation to address cyber security concerns. Many technical and network management solutions that would greatly enhance security already exist in the market place but are not always used because of cost or complexity." [16]

"The Federal government should consider options for incentivizing collective action and enhance competition in the development of cyber security solutions…Possible incentives include adjustments to liability considerations (reduced liability in exchange for improved

[13] Internet Security Alliance, *The Cyber Security Social Contract: Policy Recommendations for the Obama Administration and the 111th Congress* at 8
[14] Internet Security Alliance, *The Cyber Security Social Contract: Policy Recommendations for the Obama Administration and the 111th Congress* at 13
[15] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure* at 31
[16] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure* at 31

security or increased liability for the consequences of poor security), indemnification, tax incentives, and new regulatory requirements and compliance mechanisms." [17]

"The government, working with State and local partners, should identify procurement strategies that will incentivize the market to make more secure products and services available to the public. Additional incentive mechanisms that the government should explore include adjustments to liability considerations (reduced liability in exchange for improved security or increased liability for the consequences of poor security), indemnification, tax incentives, and new regulatory requirements and compliance mechanisms." [18]

"Mid Term Action Item #14 Refine government procurement strategies and improve the market incentives for secure and resilient hardware and software products, new security innovation, and secure managed services." [19]

WHAT IS NEEDED TO CREATE A FUNCTIONING MODEL FOR USING INCENTIVES TO SPUR BETTER CYBER SECURITY BEHAVIOR?

In order to create a system to maximize the use of market incentives for cyber security, three essential elements need to be developed.

1. A system must be developed to determine, on an ongoing basis, what voluntary behaviors will merit incentives.
2. A network of incentives must be catalogued and then applied to the widely diverse private sector.
3. A system to monitor use of the voluntary regime must be developed in order to track the appropriateness and effectiveness of the incentives.

ISA proposes a system that will address each of these areas

1. Determining what actions deserve incentives

The best way for government to motivate the specific cyber security behaviors it would like industry to adopt to meet the national (i.e. beyond normal business) interests, is to engage industry at the business plan level and make it in the private corporation's best economic interests to enhance the infrastructure.

An effective method of stimulating security would be to create a competitive market for the development and adoption of sound security practices, standards, and technologies.

---

[17] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure* at 28

[18] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure* at 31 at 8-9

[19] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure* at 37

By creating a competitive market, the power of the market can be harnessed to motivate improved cyber security and, since many of the organizations targeted are international, improvements on a worldwide basis are quite possible.

In it's testimony before the House Energy and Commerce Committee in May 2009 as well as its testimony before the Senate Judiciary Committee in November 2009, the ISA laid out the details of how such a market could be created.

ISA proposed that legislation establish the requirement for a tiered regime that would designate a family of equivalent standards (NIST, ANSI, ISO, etc) worthy of escalating incentives.

The government, as well as the private sector, would create market incentives for higher tiers of standards and practices to be utilized within businesses by designating contractual requirements that matched the criticality of a product/program to a given security posture (e.g., a contract for critical infrastructure might require a Tier 4 certification while a contract for paper products might only require Tier 1).

Such a model would provide incentives for individual companies to invest, purely on a voluntary basis, in enhanced cyber security in order to earn even higher levels of incentives.

Government's interest should not be in assuring compliance with any particular set of technologies, standards, or practices, but rather its interest should be in assuring the efficacy of the intervention. Therefore, it makes little difference how the industry meets the effectiveness levels established to qualify for an incentive (that is which standard/ practice was used to achieve the designated level), but instead, that the investments are effective in achieving a specified level of security and thus to be deserving of an appropriate incentive. .

ISA proposes that government identify multiple entities, both public and private, to identify standards and practices that would be eligible for market incentives.

Also, it is important that the government not declare a single set of standards. Government can be subject to political pressure and it can be a challenge it to deal with the vast and ever-changing array of needs that face companies, many of which are not US-based but nevertheless, actively contributing to the US economy. In addition, there may be strong international resistance to standards that are solely determined by the US government. Perhaps more important, the notion of one-size fits all does not recognize the reality of multiple business sizes, cultures, regulatory regimes, and degrees of criticality within the infrastructure and business plans.

The government's first role would be to select and fund independent research of the interventions created by the approved entities. Entities would be able to remain on the list of qualifying standards and practices only based on the efficacy of their standards as determined by independent studies.

At the outset, the ISA, proposes that companies have available federal incentives if the companies implement information security pursuant to, and meet the:

- Information security procedures adopted for regulated services by a Federal sector-specific regulatory agency.

- Standards or practices established and maintained by the organizations such as:
    - International Standards Organization
    - American National Standards Institute
    - The Internet Security Alliance
    - National Institute of Standards and Technology

- Standards established and maintained by an accredited security certification organization, or a self-regulatory organization such as NASD, BITS, or the PCI structure.

- Technologies approved as designated or certified anti-terror technologies by the Department of Homeland Security under the SAFETY Act such as DataVantage Global®.

- Private entities, such as insurance companies and audit firms, who can demonstrate either a financial interest in quality compliance or independent research.

This model has multiple advantages.

First, it allows for multiple "standards" to be rewarded and, thus, avoids the one size fits all problem of a single standard.

Second, standard-setting organizations would compete to continually improve their standards and their cost effectiveness in order to receive better grades and to qualify their users for improved incentives. The standard setting entities themselves are enhanced by the larger number of organizations that adopt their standards.

As a result, there is a built-in economic social benefit, motivated by a profit incentive that can move with far greater speed and which can easily stay abreast with ever changing technologies, their vulnerabilities and threat vectors that can the traditional regulatory mechanisms that move far too slowly to keep pace with this continuing evolution, a system motivated by the profit motive can move with far greater speed.

Third, international standards can qualify for US incentives that will better meet the needs of international corporations and will avert the potential negative issues arising from a US-only implementation or the setting of bad precedent.

Fourth, while the US cannot “govern” foreign-operating organizations, it can provide them and their US Domestic entities with incentives for good behavior thereby, allowing the US to

improve not only domestic, but also international cyber security, which is ultimately in the US' national interest.

2. *Creating a system of incentives that can be matched to various, individualized corporate needs and levels of voluntary security compliance.*

In the ISA model, various tiers of standards/ best practices could then be mapped to the qualifying incentives for these various levels of compliance (e.g. level "x" yielding tax incentive "a" and level "y" yielding tax incentive "b").

However, while it is true that one size of standards/best practices may not apply equally well to various businesses or technology systems, it is also true that one set of incentives may have different applicability and attractiveness to different types of sizes of enterprises.

Obviously, a defense contractor might be more attracted by incentives tied to government procurement, whereas a financial institution might be more attracted to insurance benefits and smaller companies might be interested in expanding the opportunity to access SBA loans etc.

As a result, ISA suggests that a range of incentives ought to be made available to those companies that choose to enhance their own security.

The following is a list of incentives, many of which are of low or virtually no-cost to the public, and can be used to alter economic perspective with respect to investment in cyber security procedures, and, thus, encourage private entities to improve their security posture in the broad national interest.

A. Create a Cyber Safety Act. The SAFETY Act, passed after 9/11 to spur the development of mostly physical security technology by providing marketing and insurance benefits, could be adapted to provide similar benefits for the design, development, and implementation of cyber security technology, standards, and practices.

By designating or certifying organizations under the SAFETY Act for developing or using cyber security technology, best practices, and standards, these organizations can similarly exploit marketing and insurance benefits, which can provide tangible business paybacks and encourage cyber security spending beyond what was justified by their initial business plans. The program has proven successful in the physical arena.

B. Tie federal monies (grants/SBA loans/stimulus money/bailout money) to adoption of designated effective cyber security standards/best practices. Using the model described above for selecting standards and practices, make on-going eligibility for federal contracts, grants and loans contingent on compliance with identified security practices. This is a proven, and successful, method for advancing broad policy objectives (e.g., non-discrimination in employment).

One of the benefits of this approach is that there is no significant impact on the federal budget due to the fact that this money is already designated for distribution. Furthermore, there is the potential for relatively immediate impact since existing standards, best practices, and government programs can be utilized and adapted to future needs since most applications must be periodically renewed. Finally, a renewal process in place for these types of government contracts will allow for compliance testing as a means of approving and of continuing the contracts. The reach of the positive effect of this approach will go beyond major players to include a broader universe of suppliers and contractors to CI/KR.

C. Leverage Purchasing Power of Federal Government. Government could increase the value of security in the contracts it awards to the private sector, thereby encouraging broader inclusion of the level of security provided to government which, in turn could facilitate broad improvement of the cyber security posture among CIKR owners and operators. The result of "building in" effective cyber security in products and services that are developed and delivered to the government at inception will not only insure to the public's best interest but if such requirements were extended to secondary suppliers and sub-contractors as well, this initiative could have a significant effect on down-stream entities as well.

While this approach does have the potential for substantial benefits, government would need to enhance the value its contracts because a number of the smaller organizations within the supply chain do not have the same massive incentive to adopt government specifications that some larger players do. While, this approach has potential for real and immediate benefits, but it is important that government realize that such compliance cannot be expected to come "for free." National security has a cost, and that cost is the government's responsibility.

D. Streamline regulations/reduce complexity. Regulatory and legislative mandates and compliance frameworks that address information security, such as Sarbanes-Oxley, Gramm-Leach-Bliley, the Health Insurance Portability and Accountability Act, along with state regimes, could be analyzed to create a unified compliance mode for similar actions and to eliminate any wasteful overlaps. Sector specific requirements could be identified, of course, but effective security has many similar elements. Duplicative regulations impose a cost on industry that ultimately increases its resistance to prioritizing compliance.

If compliance with one set of regulations were to be considered compliance with all, the reduction in compliance costs would free-up additional resources to be reinvested in cyber security initiatives, rather than in compliance efforts.

E. Tax incentives for the development of and compliance with cyber security standards practices and use of technology. Using the ISA model for selecting standards and best practices as described above, the receipt, and on-going eligibility, for tax credits can be made contingent upon compliance with established and pre-identified cyber security practices.

While tax incentives are often difficult politically, this approach may be targeted to smaller and medium-sized businesses. SMEs are a weak link in the cyber security supply chain and, without incentives, they may never perceive compliance with effective cyber security practices to be economically beneficial.

F. Grants/Direct Funding of Cyber Security R&D. The Federal Government could give grants to companies that are developing and implementing cyber security technologies or best practices. Alternatively, R&D could be run through one or more of the FFRDCs. This approach would reduce the private-sector cost of developing and deploying cyber security technologies.

G. Limit liability for good actors. The Federal Government could create limited liability protections for certified products and processes, such as those approved under the modified SAFETY Act proposal, or those certified against recognized industry best practices. Alternatively, liability might be assigned on a sliding scale (comparative liability), such as limiting punitive damages while allowing actual damages, and providing affirmative defenses with reduced standards (preponderance of evidence vs. clear and convincing etc.).

Liability costs are among the most sensitive issues confronting senior corporate executives and these costs are a long-standing target for reform. Tying adherence to best practices and standards to a limitation in liability might be extremely effective in building a business case for extended cyber security investment. There is no such thing as perfect security, but one of the biggest concerns within industry is that, despite making the best possible investments in security, a court would still impose liability for a successful, one-in-a-million hostile attack. That outcome is not in the best interest of the public policy for improving cyber security.

In making this proposal, ISA's objective is to provide incentives to those who make authentic investments in improved cyber security consistent with the standards and best practices that are incorporated into an overall government program. This objective stands in contrast to those who may argue that there should be no liability at all.

H. Create A National Award for Excellence in Cyber Security. The Government could create an award for companies that adopt cyber security best practices such as , the Malcolm Baldridge Award by the Department of Commerce.

This is a low-cost effort with substantial benefits. Organizations may strive to receive the award as a means of differentiating themselves in marketing, and consumers will most likely value companies that have this type of recognition, particularly in a marketplace in which security concerns continue to increase.

I. Promote Cyber Insurance. Cyber insurance, if more broadly utilized, could provide a set of uniform and constantly improving standards for corporations to adopt and to

be measured against, all while simultaneously transferring a portion of risk that the federal government might face in the case of a major cyber event. Insurers require some level of security as a precondition of coverage, and companies that are adopting better security practices will receive lower insurance rates. The benefits of cyber insurance and the requirements imposed by cyber insurers help companies to internalize the advantages of good cyber security as well as the disadvantages and potentially higher costs of poor cyber security, which in turn leads to greater investment and improvement in cyber security. The security requirements utilized by cyber insurers are also helpful in this regard.

With widespread acceptance of cyber insurance, these requirements will become de facto standards, while still being responsive to updates that are necessary in the face of new risks. Cyber insurers have a strong interest in greater security, and their basic requirements are continually increasing Thereby improving overall cyber security while also providing an enormous benefit in the event of a large-scale security incident.

Cyber insurance provides a smooth funding mechanism for recovery from major losses, helping businesses quickly return to normal operations and in reducing their need for government assistance. Finally, cyber insurance allows security risks to be distributed fairly, with higher premiums charged for companies whose expected loss from such risks is greater and lower premiums for companies whose expected loss is lower. This avoids a potentially dangerous concentration of risk, while also preventing companies from gaining a free-ride. Insurance companies can also provide a market-based monitoring and assessment function that reduces the cost to the government while assuring compliance with ever-increasing standards and practices.

3. A system to monitor use of the voluntary regime must be developed in order to track the appropriateness and the effectiveness of the incentives.

It is sometimes blithely asserted that if the private sector doesn't do a better job of monitoring cyber security, the government will simply have to regulate it.

Often these assertions are followed by suggestions that Sarbanes/Oxley, GLB, or HIPAA standards could simply be expanded.

Leaving aside the broad policy problems with these simple solutions, as articulated above, research suggests that such expansion of government regulation is unlikely to succeed if enacted.

The PricewaterhouseCoopers study reported in the October 2008 edition of CIO Magazine claims that only "44% of respondents say they test their organizations for compliance with whatever laws and industry regulations apply."[20] The study notes that this represents an increase in compliance, but it is extremely noteworthy that, several years after these laws and

[20] PricewaterhouseCooper, *The Global State of Information Security*, 2008

their regulations (such as HIPAA and Sarbanes-Oxley) have been in effect, less than half of the surveyed companies are even testing for compliance.

CIO magazine goes on to note, “many organizations aren’t doing much beyond checking-off the items spelled out in regulations---and basic safeguards are being ignored,” which is consistent with the findings of the 2008 Data Breach Investigations Report[21] cited earlier.

The federal government’s lack of success in getting federal agencies to meet their own FISMA requirements also suggests that this is not an area in which the federal government does well. It is impractical for the federal government, funded only by tax dollars, to take on the massive role of determining, monitoring, and constantly adjusting cyber security requirements.

Far more practical would be for the federal government to use its resources to establish a functional private sector system in which the federal government could participate and where necessary, regulate. Insurance companies are the best available vehicle for such a program.

The insurance industry is uniquely motivated to understand and communicate to its insured which standards of due care are appropriate for the management of network security because the industry has "skin in the game.” That is to say, in the event of a loss, it is the insurance company that will pay the excess of any self-insured retention and any damages to third parties, as well as reimburse the policyholder for any loss of business and any additional expenses associated with the event.

A robust cyber insurance industry, operating under traditional regulatory regimes, could best serve the public interest by providing a mechanism for the continual upgrading of security practices and standards, the monitoring of compliance, and the reduction of government’s risk exposure in the event of a cyber hurricane.

[21] Verizon Business Risk Team, *2008 Data Breach Investigations Report*

DISRUPTING ATTACKER COMMAND AND CONTROL CHANNELS: A NEW MODEL FOR INFORMATION SHARING

Information sharing is one of the most consistently discussed issues in the entire field of cyber security. Notwithstanding years of constant and often excellent work, legislative initiatives, and the creation of multiple public and private sector entities to address the problem of information sharing, there is virtual consensus that an operational model has not yet been established that provides timely, actionable, and useful information to the vast number of public and private entities who require it.

Several quotes from both the ISA Social Contract and the Administration's Cyber Space Policy Review make many of the same points.

Quotes from the ISAlliance Cyber Security Social Contract

"Starting with the organizations that already have established a priority on cyber security, we need better intelligence and information sharing for these organizations. We need to make sure the right channels are in place and approved by the lawyers. Attempting to address the information sharing issues between industry and government without involving the lawyers reflects a misunderstanding of some of our core problems and will lead to the same frustration we have had addressing this issue for years."[22]

"We need to be sure that the information being shared by our government partners can be put into action. We need to get the road blocks out of the way with respect to the timeliness of the information"[23]

"US Government entities can focus on technologies or strategies that allow members of the private sector to shift from a passive, forensics-based defense to an active posture that incorporates real-time intelligence updates that anticipate adversaries' targets and tactics. Government policymakers must combine innovative technology solutions with substantive diplomatic, economic, and policy efforts abroad to make our adversaries' operational costs and risks unacceptably high."[24]

Quotes from the Obama Cyber Space Policy Review

"Private-sector engagement is required to help address the limitations of law enforcement and national security. Current law permits the use of some tools to protect government but not private networks, and vice versa."[25]

---

[22] Internet Security Alliance, *The Cyber Security Social Contract: Policy Recommendations for the Obama Administration and the 111th Congress* at 15
[23] Internet Security Alliance, *The Cyber Security Social Contract: Policy Recommendations for the Obama Administration and the 111th Congress* at 16
[24] Internet Security Alliance, *The Cyber Security Social Contract: Policy Recommendations for the Obama Administration and the 111th Congress* at 20
[25] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure* at 17

"Some members of the private sector continue to express concern that certain federal laws might impede full collaborative partnerships and operational information sharing between the private sector and government. For example, some in industry are concerned that the information sharing and collective planning that occurs among members of the same sector under existing partnership models might be viewed as "collusive" or contrary to laws forbidding restraints on trade. Industry has also expressed reservations about disclosing to the Federal government sensitive or proprietary business information, such as vulnerabilities and data or network breaches. This concern has persisted notwithstanding the protections afforded by statutes such as the Trade Secrets Act and the Critical Infrastructure Information Act, which was enacted specifically to address industry concerns with respect to the Freedom of Information Act (FOIA). Beyond these issues, industry may still have concerns about reputational harm, liability, or regulatory consequences of sharing information. Conversely, the Federal government sometimes limits the information it will share with the private sector because of the legitimate need to protect sensitive intelligence sources and methods or the privacy rights of individuals.

These concerns do not exist in isolation. Antitrust laws provide important safeguards against unfair competition, and FOIA helps ensure transparency in government that is essential to maintain public confidence. The civil liberties and privacy community has expressed concern that extending protections would only serve as a legal shield against liability. In addition, the challenges of information sharing can be further complicated by the global nature of the information and communications marketplace. When members of industry operating in the United States are foreign-owned, mandatory information sharing, or exclusion of such companies from information sharing regimes, can present trade implications."[26]

"As part of the partnership, government should work creatively and collaboratively with the private sector to identify tailored solutions that take into account both the need to exchange information and protect public and private interests and take an integrated approach to national and economic security.

The government, working with key stakeholders, should design an effective mechanism to achieve a true common operating picture that integrates information from the government and the private sector and serves as the basis for informed and prioritized vulnerability mitigation efforts and incident response decisions."[27]

"Mid Term Action item # 8: Develop mechanisms for cyber security-related information sharing that address concerns about privacy and proprietary information and make information sharing mutually beneficial."[28]

---

[26] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure* at 18-19

[27] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure* at Executive Summary iv and v

[28] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure* at 38

TWO SOCIAL CONTACTS FOR INFORMATION SHARING

Information sharing on a national scale is dependent upon two separate social contracts. A social contract to protect the ability of the network to meet national security requirements will be quite different from a social contract for the protection of end points in industry and the general public where the threat is the loss of critical information or the unwitting participation in distributed denial of service attacks.

Major telecom providers and networking equipment providers have a social contract to maintain the Internet for the good of the nation from both a national security and national economy viewpoint. At times these two goals will be at odds with each other, as the mitigation of a network denial of service attack aimed at our national security would have serious economic impact. As such, the greater the level of precision that can be applied in any situation, the lesser the impact to our economy. Information sharing in this environment must be targeted at macro network traffic. Information sharing provides a mechanism for understanding what is normal on the network, for recognizing sudden or gradual changes, and for working with industry partners and government to react to an attack. The government structure to support information sharing for this social contract is already in place through the National Communication System. It should be expanded with appropriate legal protections for those who are sharing their network information and are taking actions at government direction.

C2 DISRUPTION STRATEGY – A SOCIAL CONTRACT FOR COMMERCIAL, GOVERNMENT, AND PRIVATE END USERS

ISA proposes for consideration a different model of information sharing which attempts to address some of the concerns expressed in the opening comments to this section. Specifically, we believe the ISA model below takes a differentiated approach which appreciates that there is not a one size fits all solution. In addition, the ISA seeks to overcome the inordinately low participation rates from the private sector in the various information sharing organizations (such as the ISACs), which is not, primarily, due to a lack of awareness, but, rather, to a lack of corporate resources to utilize these fine services. Further, ISA believes that the proposed model will help to resolve some of the legal and lack-of-trust issues that are present in both the public and private sector players by altering the nature of the information that is to be shared. Finally, ISA model proposes to utilize a series of market incentives to motivate participation and use of the system.

The information sharing that is required to support a social contract between the government, commercial enterprises, and private end users will look quite different from the contract for network providers. The objective of the ISA social contract is to provide end users the means to both protect their intellectual property and to be good network citizens by not contributing to malicious network traffic. With the possible exception of critical infrastructure industries, the government has no vested interest in obtaining from the public anything more than a statistically significant sample of network events. Indeed, anything greater than a small snapshot of activity from end users would overwhelm any conceivable ability of the government to digest the information. This is not to discount the value of information sharing

within critical sectors in a model based on the Defense Industrial Base effort, but ISA does not believe that that model is scalable on a national level.

Instead, any information sharing model involving anyone beyond the largest government and industrial enterprises must recognize that the vast majority of organizations and individuals can only be on the receiving end of the information flow. They simply haven't made the investment necessary to have the skills in place to either produce information worth sharing or to make appropriate decisions when presented with detailed threat information. The implications are that to be effective on a national scale, any information that is shared has to be available to, and actionable by, even those with the most limited cyber defense investment .

This is a tall order, but we believe that there is an opportunity for us to meet this challenge and to raise the information assurance posture of the entire nation—government, industry, and the public—by instituting a process to identify and block, on a wide scale, the command and control links of botnets, advanced persistent threats, and criminal malware. By instituting such a C2 Disruption strategy on a broad scale, it's possible to disrupt the ability of malware to communicate with its controllers and many of today's threats.

UNDERSTANDING THE NATURE OF THE MODERN PROBLEM

In today's cyber security environment, there is one inescapable truth: there is no way to consistently prevent a determined intruder from getting into a network so long as one allows e-mail and web surfing, and no business or agency operating today can long survive without these two bedrocks of the information age.

The reasons for this are simple. The vast majority of our Information Assurance architectures rely on patching and configuration control for protection, the consistent application of which has thus far proven elusive over large enterprises. The architectures also rely on signatures for both protection and detection which, by definition, will not stop the first wave of the increasing volume of zero-day attacks we are seeing today. Therefore, when you must let the attack vector (an e-mail or a web address) past your perimeter to the desktop, you are virtually guaranteed to have successful penetrations.

Perhaps the best way to address this new reality is to recognize that attackers will get into your network and to expand defensive actions to detect, disrupt, and deny an attacker's command and control (C2) communications back out to the network. It is an acknowledgement of the fact that there are fewer, or perhaps relatively noisier, ways to get out of a network than to get into it. Such a strategy focuses on identifying the web sites and IP addresses that attackers use to communicate with malicious code that has already infiltrated into our computers. While some of these sites are legitimate sites which have been compromised, the majority of the sites are usually new domains registered by attackers for the sole purpose of command and control.

There is little danger of unintended consequences from blocking these web sites and their associated IP addresses for outbound traffic. Where they are legitimate sites, the benefit of protecting the enterprise far outweighs any inconvenience that might arise if an employee

needs to legitimately go to a site. Some larger organizations have had success with this strategy, but the strategy requires a significant investment, unaffordable to most small and medium size entities and, even, many larger ones.

One of the corollaries of recognizing that networks can always be penetrated is a shift in how we measure our own defenses. Measuring these defenses against how many intrusions occur is no longer the most important criteria. What counts, instead, is the intruder's dwell time in a network, or how long an intruder has had access to our network. It is more important to recognize how successful the penetrations were versus how many penetrations occurred. The ideal goal would be to have advance notice of a new malicious C2 channel so that even if someone opened a malicious e-mail the outbound C2 channel would already be blocked—making the effective dwell time zero.

ISA believes that the most effective way to reduce dwell time is a method that every organization, large and small, can match, collaboration with other operational entities. We recognize that many other organizations regularly find and report C2 channels. Anti-virus vendors, CERT CC, managed security service providers, defense contractors, research institutions, intelligence agencies, other large government agencies, and law enforcement all see relatively narrow aspects of the C2 environment. But put them all together and they collectively see a very wide swath of the C2 threat environment. Many already aggregate and share the information formally, or informally, through ISACs, the Defense Industrial Base Cyber Task Force, Infraguard, along with a number of other forums. However, there is no central clearing house for this information, nor is there an operationally focused framework for rapid dissemination of this threat information to a broad national audience.

It is in this collaborative realm that there may be an opportunity for a national-scale effort that can turn collective effort to our advantage in the cyber battle. The gaping hole in cyber collaboration (often called information sharing) is that the vast majority of small-, and medium–sized organizations, neither commercial and government, do not participate in these groups, nor do they have the resources to take advantage of this information when they get it.

While there is no national-scale framework in place for collaboration on C2 Channels, there is a model that has already proven effective in fighting other cyber security problems. The model involves a set of trusted entities that develop threat information and report voluntarily (with non-attribution) to a central source, which then consolidates the information and rapidly disseminates the information to a very large user community. The user communities, in return, implicitly trust the centralized service and expend little or no resources to validate the information. The communities simply let the automated processes protect them as a passive service rather than investing in active collaboration—all with much better results.

If this sounds familiar, it's because this is the model used by the highly successful anti-virus and spam filtering industries. We propose to use the same model to disseminate information on attacker C2 URLs and IP addresses and, then, automatically block <u>outbound</u> traffic to these addresses. If attackers get into your network but cannot get back out, attacks are effectively thwarted.

Such a model will have a tremendous impact against botnets and advanced persistent threats, both of which make heavy use of web-based command and control. While the first wave of attacks might initially succeed, they would be short-lived after the first discovery because of the rapid, automated dissemination of the C2 channels. Subsequent waves would fail completely by virtue of this rapid dissemination and automatic blocking of the C2 mechanisms. Of course, one could argue that an attacker could always rapidly change their command and control channels and make the channels unique to each attack. While this is true, the more we force intruders into greater costs and complexity, the more likely we are to change their cost-benefit calculations. It seems axiomatic that anything that is both simple and inexpensive in forcing this behavior is worth doing on our part.

ISA proposes a model for establishing a National Cyber Threat Protection Service to implement a C2 disruption strategy. The model will describe the process, key relationships, the responsibilities of the participants and the incentives for each community of interest. This would be a voluntary model. Within all of the communities described below, not everyone has to participate for the model to be effective. The more who participate the better, but the benefits will quickly accrue to a wide swath of both the public and private sector after the process includes a critical mass of participants.

AN INDUSTRY-GOVERNMENT COOPERATIVE MODEL FOR DISRUPTING MALICIOUS CYBER COMMAND AND CONTROL

There are three types of entities involved in this process:

1. **Threat Reporters** who discover and report malicious C2 channels.

2. **A National Cyber Threat Response Center (NCTRC)** which acts as a central threat clearing house, collecting the threat reports, vetting them as necessary, and providing them to vendors in a standard format.

3. **Firewall Devices Vendors** (the term here being used in its most generic sense) who would accept the new threat information and push it out to their devices in the field the same way anti-virus and spam filtering vendors push new definitions today.

Certified Threat Reporters

Threat Reporters are organizations with the detection and analytical capability to discover command and control sites via malware reverse engineering or via traffic analysis. Organizations, be they commercial, private, or governmental, would apply to be certified as Threat Reporters and, through the certification, have their reports of C2 channels be accepted as valid.

Some third party, presumably a government entity, an industry consortium or some hybrid of the two, would be responsible for certifying potential Threat Reporters against a moderate standard of in-house capabilities. The standard would measure both quality and quantity of reports. Quality would be evaluated by a review of in-house detection and analytical

capabilities designed to give *a priori* confidence in the reports' reliability. This would ensure that the information provided by the reporters is credible and will allow for a more rapid automated dissemination process with minimum manual review. Quantity would be measured after certification to ensure that the reporter contributes enough unique threat information to the community to continue to merit the marketing advantage gained by being a Certified Threat Reporter.

It is important to note that submission of reports by Threat Reporters would not be the same as the disclosure of breaches as required under other laws or agreements. A significant percentage of reports would come from intelligence or from other detection activities not associated with any activity within the reporting organization's network. For this model to be viable, the reporters have to be free to provide threat information without any implication that they experienced a breach or that they might get requests for involuntary disclosure of additional information.

Threat reporters would normally submit only malware command and control information, either web sites or IP addresses, as well as the class of threat (e.g. botnet, advanced persistent threat, etc). That information alone is enough to make this model work if all parties trust the credibility of the assessment. Other detailed information on the malware involved could be voluntarily submitted, but not at the expense of rapid submission of the C2 channels.

The advantage to the Threat Reporters, especially managed security service providers, is in the ability to use the certification for branding purposes. Organizations that develop threat data internally, but which do not wish to participate due to low risk tolerance or because they feel reporting might conflict with their business model, would simply not apply to become Threat Reporters.

National Cyber Threat Response Center (NCTRC)

The role of the NCTRC is to serve as a clearing house for processing reports of C2 URLs and IP addresses from Threat Reporters and to rapidly distribute the reports to the community of firewall device vendors. By having a central point disseminating the information to all vendors equally, the problem, where not all vendors detect all threats can be avoided. The NCTRC would also de-conflict all erroneous reporting that resulted in disruption to legitimate activities. The NCTRC would maintain a "reputation index" (e.g. credibility rating) for each reporter much like seller ratings on eBay. Through this feedback loop, a Threat Reporter could be decertified (i.e. no longer have their reports accepted and no longer be able to claim Threat Reporter status in their marketing).

The NCTRC must be a single organization focused on rapid dissemination of actionable information. Unlike the current anti-virus business model, where organizations submit malware to their vendor of choice, there would be only one clearing house in this model. The question of who operates the clearing house is largely irrelevant, so long as everyone in the model trusts that entity. It could be a government entity or, more likely, a non-profit organization overseen jointly by the government and an industry consortium. Regardless of who operates the NCTRC, the government must be as secure in reporting information to it as industry is. With the large amount of IP threat information that the government sees simply

because of the size of its network, the absence of threats detected in government's networks would significantly reduce the value of the model.

Firewall Device Vendors

Producers of devices that are capable of blocking outbound web traffic would accept the data from the Clearing House, re-format it as appropriate for their device, and, then, push the information out to their customers as quickly as possible. Traditional desktop or network firewalls, web proxies, and routers would all be capable of performing this function, thereby giving network owners a wide variety of products from which to select based on their architecture and their investment tolerance. The vendors would differentiate themselves from each other not only on price, but also on the speed of updates and value-add services, such as the ability of their customers to manually override the lists, or the ability to provide reports to network owners.

Industry, Critical Infrastructure Providers, and Government

The real benefit from this model lies with the vast majority of network owners in business, industry, and government who cannot afford the deep detection and analytical capability needed to protect themselves. Today, these organizations are totally at the mercy of a determined intruder who is virtually guaranteed to be able to compromise systems with socially-engineered zero-day attacks. Most network owners simply do not have the investment dollars to build a detection infrastructure that is dependent on traffic analysis, nor do they have the expertise to make use of the various information sharing groups. With this model, though, however these businesses could easily, and voluntarily, afford a single device that most users already have

The model would, however, therefore provide an order of magnitude increase in the level of protection by stopping, in near real- time, many of the paths an attacker would use to escape from the network. For those network owners who had not yet been compromised when updates were released, the updates would completely nullify any subsequent attack with that command and control channel. For those who had already been compromised in the first wave of a zero-day attack, the updates would minimize the length of time when an attacker could access the compromised box, and they would identify compromised computers that might have otherwise gone undetected. Best of all, assuming that they implicitly trust the system, the organizations that employ the model do not have to invest any additional resources to take full advantage of the model.

A secondary benefit would accrue to organizations whose websites have been hijacked and are being used as C2 sites (as opposed to dummy domains registered specifically for C2). These organizations would become aware of the infection more quickly as hits on their web sites dwindled or as they monitored the NCTRC lists. The organizations would be then able to exhibit good internet citizenship by quickly cleaning their systems and by working with the NCTRC to be removed from the block list.

A third benefit, although perhaps more appropriate as a follow-on effort, would be the ability to tie the reported C2 channels to a library of instructions for finding and cleaning the specific malware where is was detected. This would be a much more complex and a less automated

process, but it would give smaller organizations a quick way to not only know they have a problem, but also allow them to short circuit the remediation process.

THE PROSPECT OF A COMMON OPERATIONAL PICTURE

Perhaps one of the most tantalizing side benefits of this model is that it could serve as the basis of a true Common Operational Picture (COP). If every firewall device that supported this model not only blocked the outbound traffic, but also—again, voluntarily—reported back to the NCTRC that there was a blocked C2 attempt emanating from their IP address, it would, given the potentially hundreds of thousands of devices reporting in, represent a very accurate picture of the scope of any given attack or campaign. Unlike today, when organizations are loathe to reporting incidents because of the risk of bad publicity, data reported to this COP would not reveal any information beyond the fact that someone on the an organization's network tried to communicate with a bad URL or IP. Plus, by definition, if the firewall device blocked the outbound traffic, the attack failed or was neutralized. Additionally, knowing the nationwide scope of attacks from the same source would yield invaluable information unavailable today.

If the IP addresses reporting in could be grouped by their critical infrastructure or agency, the COP could be filtered to that organization. For example, if the NCC knew the IP space of all nuclear power plants, a COP could show attempts to access the same C2 sites from multiple power plants. This might indicate a concerted effort to compromise the plants. Similarly, the defense industry or the financial community could see the scope of attacks across their community. Or, the Department of Defense could see which attacks were unique to their network, since there may be no detections of specific C2 sites outside of DoD IP space. And, all of this could occur in near real-time.

INCENTIVES

This model for denying and disrupting attacker command and control on a national scale includes positive incentives for every participant.

1. Organizations, especially commercial entities, will have an incentive to become Certified Threat Reporters for branding purposes. It would demonstrate that they have a robust, capable process and investments to become credible reporters of threat data. There could even be, for branding purposes, tiered levels based on the volume and accuracy of inputs. For example, an anti-virus vendor who might report a lot of C2 URLs based on all the malware could become upgraded to a they get would be Platinum Certified Threat Reporters. A large company with robust internal capabilities might be achieve Gold level. Managed Security Service providers would be especially eager to participate since the number of C2 channels first reported by such providers would be a tremendous marketing tool for them.

2. The Government will greatly benefit by being provided with a very large body of C2 URLs and IPs for very little investment on their part. They will also benefit, of course, by the overall increased security of the industrial base, which is a major goal of US policy. Most important, however, is the promise of a near real-time common operating picture that truly reflects the current threat environment. The main burden on the government's part would be the up-front effort to champion implementation and to develop interface standards for receiving reports and disseminating them to vendors.

3. Firewall Device Vendors will have a great incentive to participate. They will be noticeable by their absence if they don't participate, and it will most likely open up a whole new class of customers who will recognize, in a single device, a high-payoff, defensive measure.

4. Best of all, small- and medium-sized organizations of all types will now have a way to take collective advantage of the investigative work of the best Information Assurance organizations in the country. By investing only in the firewall device that best fits their architecture, their security will increase by an order of magnitude, or, more simply because, like AV, a known bad domain will get blocked within hours of discovery.

5. This model would also help to restore trust in the Internet by identifying and isolating ISPs that do not maintain standards of good behavior on their networks. Their IP space and registered domains would frequently be blocked, presumably reducing their profitability and providing an incentive to establish good behavior.

6. Once this model is up and running, it could easily be extended internationally. In fact, many foreign producers would have a great incentive to make their devices capable of participating in this model. From there, it would be a short jump to an international model.

RISKS

The main risk associated with this model is the risk of blocking a legitimate web site that has been overtaken by an attacker for use as a Command and Control site or as a downloader site. While we believe this risk will be small compared to the gain, the model envisions a reclaim or de-confliction process, whereby a domain owner could get his domain removed from the list, either by proving a reporting error or by demonstrating that his site was no longer hijacked. A secondary mitigation would be for the vendors to allow manual overrides on

blocked domains at the local level, exactly as it is done today, with exceptions to web proxy vendors' predefined categories.

There is a secondary risk involved in building the trust relationships required to make this model work. Industry and government alike must be assured that there is no negative connotation to submitting threat data. The simple imperative of getting malware command and control data out to the broadest possible audience must take precedence.

SUMMARY

The ISA model, if implemented on a national scale, has the potential to be a game changer. For every attack, if only one organization discovered the attack, the entire nation would be protected soon thereafter. The model would force an attacker to make the command and control channel unique for every attacked IP address. An attacker would have to either reduce the scope of attacks, or greatly expand his domain registrations. In the latter case, someone who registers enough domains to operate on the level on which our attackers operate today would soon gain such a high profile that they would be susceptible to other mitigations.

In the end, the ISA model takes the best aspects of today's anti-virus, spam filtering, and proxy URL categorization to build a fourth service that is akin to anti-virus on outbound traffic. This National Model for Disrupting Attacker Command and Control could set a new standard for effective public-private partnership in the Internet Age.

ORGANIZING FOR CYBER SECURITY:
AN ENTERPRISE EDUCATION PROPOSAL

THE NEED FOR AN ENTERPRISE EDUCATION PROGRAM ON THE FINANCIAL MANAGEMENT OF CYBER RISK

Education has been widely discussed as one of the key elements of a comprehensive and sustainable cyber security strategy. At some point, almost every public official who addresses the issue of cyber security stresses the need to include cyber training in K-12 education and, often, highlights the need to expand higher education programs in cyber security. In many instances, these officials also note the need to upgrade the cyber expertise of the federal workforce.

While ISA agrees with those sentiments, we note that one of the most critical areas of education currently lies in the enterprise arena.

The current private sector workforce, most of which will remain working for decades to come, is largely uneducated about cyber security. For the most part, the people in this group (especially senior executives) are what demographers are now calling "digital immigrants." Digital immigrants, as opposed to today's teenagers and, younger, "digital natives" were not born into the world of digital media that now surrounds them and comprehensively affects their lives. This enormous executive and non-executive workforce are on the front lines of today's cyber wars, and they are largely unfamiliar with, and sometimes inhibited by, the weapons we will all need them to use in our collective defense.

Also, perhaps more importantly, corporate leadership is structured in such a way that the real financial issues it faces with respect to cyber security are masked. As a result, cyber threats are not only under realized, but funding decisions are also confused and proper defense is compromised.

If, as it is widely believed, 85% of our cyber systems are in corporate hands, then the need for a substantial Enterprise Education program to address workplace, as well as senior management structural issues, must be given a higher priority than it currently receives.

ISA STATED POSITION

We do not have a common risk framework that helps organizations to understand the various risks that a cyber security incident represents, or that provides a roadmap for how to maximize ROI on cyber expenditures by using an enterprise risk management paradigm.

From a corporate perspective, cyber security is still too often perceived as simply an IT cost center rather than an enterprise-wide risk management issue with serious financial implications. The silo-specific view of cyber issues, which is fueled by antiquated corporate

structures and attitudes, results in an insufficient analysis of the true needs and values associated with cyber security.[29]

Modern corporations are inherently integrated by modern technology. Yet, unfortunately, corporate structures and decision-making has largely retained a 19th/20th century model of independent departments and silos that does not facilitate appreciation of the interdependency that is, today, and a corporate fact of life.

To date, a practical methodology has not been developed that corporations can easily use to addresses the risks and the potential financial losses created by the lack of appreciation of this interdependency.

Corporations need to truly understand the financial impacts of insufficient cyber security. In addition, they need to enact management systems, directed by their CFO's, which bring everyone to the table to address cyber security issues on an enterprise-wide basis. This process would involve security and technology personnel, but these groups would not be in charge of cyber risk management. An enterprise-wise structure must include, at minimum, financial, legal, operational, human resources, communications, public policy, investor relations, compliance, risk management and senior corporate officials.[30]

OBAMA ADMINISTRATION VIEW

President Obama recognized this problem, and he pointed to a new direction by which to address it when he spoke at the White House on May 29, 2009:

"It is not enough for the information technology workforce to understand the importance of cyber security; leaders at all levels of government and industry need to be able to make business and investment decisions based on knowledge of risks and potential impacts."[31]

"If the risks and consequences can be assigned monetary value, organizations will have greater ability and incentive to address cyber security. In particular, the private sector often seeks a business case to justify the resource expenditures needed for integrating information and communications system security into corporate risk management and for engaging partnerships to mitigate collective risk. Government can assist by considering incentive-based legislative or regulatory tools to enhance the value proposition and fostering an environment that encourages partnership."[32]

---

[29] Internet Security Alliance, *The Cyber Security Social Contract: Policy Recommendations for the Obama Administration and the 111th Congress* at 8

[30] Internet Security Alliance, *The Cyber Security Social Contract: Policy Recommendations for the Obama Administration and the 111th Congress* at 9-10

[31] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure* at 15

[32] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure* at 18

INDEPENDENT RESEARCH VALIDATES THIS PERCEPTION

The ISA/Obama perception is validated by the findings of the PricewaterhouseCoopers 2008 Global Information Security Survey which found that:

"The security discipline has so far been skewed toward technology—firewalls, ID management, intrusion detection—instead of risk analysis and proactive intelligence gathering. Security investment must shift from the technology-heavy, tactical operation it has been to date to an intelligence-centric, risk analysis and mitigation philosophy... We have to start addressing the human element of information security, not just the technological one, it's only then that companies will stop being punching bags."[33]

To be sure there have been steps already taken in this direction. For example, the finance sector has federal, state, and international regulatory requirements that must be met and assessed with regard to risk to information system and IT infrastructure and take steps to remediate identified risks. Reporting to the Board is required as are reports to be made to chief risk officers and chief compliance officers. Additionally, threats are examined beyond the individual firm through collaborative efforts on the part of the sector ISAC, the SCCs, and the public/private partnerships that have evolved in these sectors. Some other sectors of the economy have made similar preliminary steps.

However, the general picture regarding the financial management of cyber risk is less encouraging. The Carnegie Mellon University (CMU) CyLab 2008 Governance of Enterprise Security Study concluded: "There is still a gap between IT and enterprise risk management. Survey results confirm the belief among IT security professionals that Boards and senior executives are not adequately involved in key areas related to the governance of enterprise security."[34]

The CMU study provided damning details about the state and the structure of enterprise risk management of cyber security. The study pointed out that only 17% of corporations had a cross-organizational privacy security team. Less than half of the respondents (47%) had a formal enterprise risk management plan, and, in the 1/3 of the 47% that did have a plan, IT-related risks were not included in the plan.

Further confirmation of this problem was provided by Deloitte's 2008 "Enterprise Risk" study, which concluded that 75% of US companies do not have a Chief Risk Officer. The Deloitte study went on to document that 65% of US companies either do not have a documented process through which to assess cyber risk, or do not have a person in charge of the process they currently have in place (which functionally translates into having no plan for cyber risk at all)[35].

[33] PricewaterhouseCooper, *The Global State of Information Security*, 2008
[34] CyLab, *Governance of Enterprise Security Study*, December 2008 at 1
[35] Information Security & Enterprise Risk 2008, Presentation to CYLab Partners Conference, Delloite, Carnegie Mellon University, Pittsburg, PA, October 15, 2009

In 95% of US companies, the CFO is not directly involved in the management of information security risks.

A GROUNDED APPROACH TO BUILD AN ENTERPRISE EDUCATION PROGRAM

In 2008, ISA recognizing these trends in conjunction with the American National Standards Institute (ANSI), launched a broad-based program aimed at elevating and expanding the cyber security field. The program resulted in the publication of the landmark action guide for the enterprise space, "The Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask"

This publication provides the ideal template to use to quickly and effectively create an enterprise education program.

The ISA/ANSI program was continued in 2009, and it was expanded to create a second publication that will provide responses and frameworks for use in addressing the questions that were raised in the original document. Release of the second publication is expected in early 2010.

THE ISA/ANSI TASK FORCE ON FINANCIAL CYBER RISK TAKES A MULTI-DIMENSIONAL APPROACH TO ANALYZING AND ADDRESSING CYBER RISK

From May 2008 through October 2008, ISA and ANSI established a Cyber Risk Task Force and held a series of conferences to evaluate the state of enterprise cyber risk management and to determine how to address any problem areas that were revealed by the analysis. The Task Force concluded that, "Unfortunately, corporations have often failed to properly account for the financial downside resulting from the risks of cyber systems."

Corporate America cannot be completely faulted for this deficiency, since, to date, there has not been any agreed upon methodology for understanding and mitigating the potential financial losses associated with network security and cyber risk. The financial risk management discipline that Chief Financial Officers and Risk Managers have classically used to deal with brick-and-mortar risks has not yet been systematically applied to digital risks.

While there is a substantial body of work that deals with the technical standards of network, Internet, and computer system security, and while plenty of attention has been paid to important issues such as data encryption and best-in-class security technologies, classic financial risk management— as it pertains to cyber security exposures—has been largely overlooked.

The purpose of the ISA/ANSI work was to correct that deficiency by providing guidance in both the identification and quantification of the financial risk caused by issues related to information security.

The key to understanding the financial risks of cyber security is to fully embrace its multidisciplinary nature. Cyber risk is not just a "technical problem" to be solved by the

company's Chief Technology Officer, and it is it not just a "legal problem" to be handed over to the company's Chief Legal Counsel. Similarly, cyber risk is not just a "customer relationship problem" to be solved by the company's communications director, nor is it just a "compliance issue" for the regulatory guru, nor is it just a "crisis management" problem.

Rather, cyber risk encompasses all of these problems, and more.

Successful analysis and management of financial risk requires a dialogue, sparked by a series of pointed questions directed to the major stakeholders in all corporate domains: the Chief Legal Counsel, the Chief Technology Officer, the Chief Risk Officer, along with the heads of Corporate Communications, Investor Relations and Customer Service. Each of these individuals should be "in the room," along with a surprised CFO who discovers that individuals with different positions in the company give very different, sometimes contrary, answers to the same question.

The Financial Impact of Cyber Risk produced by ISA/ANSI[36] is an action guide and offers practical, immediately-actionable guide on how to bring together the multiple stakeholders in cyber security, and how to give them, in the form of strategic questions, a roadmap for developing a multi-disciplinary risk management approach to analyze, manage, and mitigate the financial risks of cyber security. The answers to these questions will better enable a company's CFO to determine the company's "Net Financial Risk."

As companies study the questions posed in this work, they will find that the answers can be plugged into the formula below, enabling the companies to better quantify their own net cyber risk. However, it is important to understand that the quantitative evaluation of these factors (Threat, Consequences, and Vulnerability) must be qualified by the degree of confidence that the organization has in the accuracy of each factor. Once the risk equation has been qualified by the degree of confidence, it will provide a sound basis for guiding all risk management decisions.

NET FINANCIAL RISK FORMULA
THREAT x CONSEQUENCES x VULNERABILITY – RISK TRANSFERRED = NET FINANCIAL RISK

STRATEGY AND TACTICS FOR THE ISA ENTERPRISE EDUCATION PROGRAM ON THE FINANCIAL MANAGEMENT OF CYBER RISK

STRATEGY

ISA and ANSI have already analyzed and determined which key issues/questions ought to be raised in the context of a collective and ongoing process that is geared to assess, and to mitigate, net financial risk.

[36] ANSI/Internet Security Alliance, *The Financial Impact of Cyber Risk: 50 Questions every CFO Should Ask*, 2008

The next step will be to construct an enterprise education program around these principles that is suitable for dissemination, either via corporate on-site sessions, seminars at professional conferences, or webinars.

ISA and ANSI have embarked on phase II of this project, which is designed to develop individualized tools to address unique financial cyber security issues from a multi-dimensional perspective.

By addressing cyber security through the perspective of an enterprise's own core goals and objectives, ISA proposes to provide a greater incentive for the enterprise to appreciate and address the issues of cyber security.

By leveraging the financial well-being of the enterprise itself, as opposed to an appeal to national pride or collective security, ISA believes that pragmatic improvements can be expected (and can be continued) irrespective of the global macro-, or micro-financial environment.

Through this pragmatic approach to enterprise cyber security, ISA believes it can create a sustainable system of security that spans the international reaches of the enterprise space and adheres to overall national security since the vast majority of critical cyber infrastructure is in private hands.

TACTICS

Below are lists of ten questions/issues that, as determined by the ISA/ANSI Cyber Risk Task Force, would be most useful to address in this context. These questions serve as the core of the individualized, yet integrated perspectives that must be addressed to fully appreciate and address enterprise-wide cyber security.

Key Questions for the CEO and Directors

1. Has senior management established an appropriate information and internet security policy and auditing process?
2. Is security viewed as an overhead activity or as essential to business survivability?
3. Are security considerations part of our normal business processes?
4. Do managers at each level of the organization understand their roles and responsibilities with respect to information security?
5. What are the organization's most important security policies and what business objectives do these policies satisfy?
6. What is your role in ensuring security policies are followed?
7. How does the organization identify critical information assets and the risk to these assets?
8. Are critical information assets managed in a similar fashion to other key business risks? What are the primary components of the organization's security architecture and what business objectives does the security architecture satisfy?

9. Do we have a process for linking new assets into our overall security system?
10. How do we integrate the security of partners, clients, and vendors to assure our own corporate security?

Key Questions for the Chief Legal Counsel

1. Have we analyzed our cyber liabilities?
2. What legal rules apply to the information that we maintain or that is kept by vendors, partners and other third parties?
3. Have we assessed the potential that we might be named in class action lawsuits?
4. Have we assessed the potential for shareholder suits?
5. Have we assessed our legal exposure to governmental investigations?
6. Have we assessed our exposure to suits by our customers and suppliers?
7. Have we protected our company in contracts with vendors?
8. What laws apply in the different states and countries in which we conduct business?
9. Have we assessed our exposure to theft of our trade secrets?
10. What can we do to mitigate our legal exposure and how often do we conduct an analysis of it?

Key Questions for the Compliance Officer

1. Have we inventoried what regulations with which we must comply?
2. Do we understand what regulated data we have, where it exists, and in what format?
3. Are there valid business reasons for collecting the data, if not required by regulations?
4. How do we track and monitor compliance on an ongoing basis?
5. Do we have regulatory risk with vendors / companies we do business with?
6. Are all of our procedures and policies in line with respect to our regulatory obligations?
7. Are there (regulatory) requirements we can, or have considered opting out of?
8. Are there processes and procedures in place regarding data retention and data destruction?
9. Does the organization have processes to review and update privacy policies and disclaimers to customers?
10. Are we complying with what our privacy policy says?

Key Questions for the Business Operations and Technology Teams

1. What is our biggest single vulnerability from a technology or security point of view?
2. How vulnerable are we to attack on the confidentiality, integrity, and availability of our data and our systems?
3. If our system goes down, how long until we are back up and running, and are there circumstances where we do NOT want to be back up quickly?
4. Where do we stand with respect to any information security/technology frameworks or standards that apply to us?
5. Do we have the proper staffing to reasonably maintain and safeguard our most important assets and processes?

6. What is the assessment of physical security controls at each of our sites (data center, home office, field offices, and other sites?)
7. How prepared are our incident response and business continuity plans?
8. What is our risk exposure of technology or business operations failures at our vendors and service providers?
9. What is the maturity of our information classification and management program?
10. How often are we re-evaluating our technical exposures?

Key Questions for the External Communications and Crisis Management Teams

1. Do we fully understand the overall financial impact of mishandling communications with our key stakeholders following a cyber security event?
2. Have we evaluated the appropriate communication responses to our key stakeholders?
3. Do we have a documented, proactive crisis communications plan?
4. Have we identified and trained all of the internal resources required to execute the communications plan?
5. Do we have a template timeline for executing the communications plan?
6. Do we have contacts at specialist crisis communications firms if we need their services?
7. In the case of a cyber security event involving personally identifiable information (PII), do we have a system in place to quickly determine who should be notified, and how?
8. Have we considered that, depending on the situation, we may need to craft different messages for different types or levels of clients or employees?
9. Have we implemented improvements as a result of an actual execution (real or mock) of the plan?
10. Have we budgeted for a cyber security event?

Key Questions for the Risk Manager for Corporate Insurance

1. Doesn't the company already have insurance coverage for this?
2. What does cyber risk insurance cover?
3. What types of cyber security events are covered by this insurance, and how are our insured losses measured?
4. Does the policy specifically cover identity theft issues?
5. Is there a Directors' & Officers' exposure if we do not purchase the cover?
6. Where do we find an insurance broker who can assist in evaluating whether we need this type of insurance?
7. How do we know what insurance carrier to consider with respect to this insurance?
8. Have there been losses in this area?
9. What does a policy cost?
10. What are the other benefits of our purchasing a specific cyber risk insurance policy?

Key Questions for the Human Resources Head to Manage Insider Threats

1. Do we periodically conduct awareness and training for all employees in cyber security?
2. How strict are our password and account management policies and practices?
3. Are we logging, monitoring, and auditing employee online actions?

4. What extra precautions are we taking with system administrators and privileged users?
5. Do we use layered defense against remote attacks?
6. Are we able to monitor and respond to suspicious or disruptive behavior?
7. Do we routinely deactivate computer access following employee termination?
8. What are our practices for collecting and saving data for use in investigations?
9. Have we implemented secure backup and recovery processes?
10. Have we clearly documented insider threat controls?

ADDRESSING INTERNATIONAL ISSUES IN CYBER SECURITY

ISA was established in 2001 on a unique model - the same model as the Internet. ISA represents companies from multiple economic sectors because the challenges with Internet security affect all sectors and, indeed, many modern corporations also transcend these artificial and theoretical structures.

From inception, ISA has welcomed international members, and 2 of its 5 Board Chairs are from European nations. This is due to the fact that ISA recognizes that cyber security is, inherently, an international problem and must be addressed on a global basis. Unfortunately, traditional nation-state boundaries may further complicate the creation and the implementation of effective cyber security solutions due to nation-states' individual and entrenched legalistic and regulatory structures.

Realizing that cyber security is a 21st century problem that will require novel solutions, ISA is endeavoring to use the multi-national operations of the private sector to breakdown the borders that the Internet as a technology has never recognized.

Effective network and infrastructure security is essential to ensure the confidentiality, availability, and integrity of the national and global information networks upon which the United States increasingly depends upon for essential services, economic stability, and economic security. The issue to be addressed is how nations can act both individually and communally to enhance network and infrastructure security and to prevent debilitating attacks by organized cyber criminals, hostile nation-states, or non-state actors.

Organized criminals, individual hackers and non-state actors, and, potentially, terrorists pose some of the key threats to public and private sector cyber security. The most costly threats to the integrity and availability of both national and global information infrastructures originate overwhelmingly from revenue generating criminal activity, not from military cyber attacks by nation-states.

Foreign intelligence services have discovered that unclassified U.S. government and private sector information, once unreachable or once requiring years of expensive technological or human asset preparation to obtain, can now be accessed, inventoried, and stolen with comparative ease through the use of computer network operations tools. The return on investment for targeting sensitive U.S. information (the intelligence gain) can be extraordinarily high, while the barriers to entry (the skills and technologies required to implement an operation) are comparatively low. Many countries are in the process of developing capabilities either to respond defensively to this threat, or to build their own offensive network operations programs. U.S. officials are increasingly willing to publicly acknowledge that these types of network exploitation and intelligence collection activities are some of this country's key counterintelligence challenges.

U.S. Government officials assess that this activity, in the aggregate, has the potential to erode the United States' long term position as a world leader in Science & Technology (S&T) innovation and competitiveness. In addition, the collection of U.S. defense engineering data

has possibly saved the ultimate buyer of this information years of R&D and significant amounts of funding.[37]

The 2007 Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, published by the National Counterintelligence Executive, noted that the U.S. remains the prime target for foreign economic collection and industrial espionage by virtue of its global technological leadership and innovation.[38] The methods employed by data collectors include direct requests, solicitation and marketing of services, and the targeting of U.S. travelers overseas. The threat is both state-sponsored and espionage-focused. It is a criminal business with low entry costs and potentially high return on investment.

Increasingly, data collectors make use of technologically-sophisticated methodologies, such as cyber attack and exploitation, which obfuscate their identities and goals.

More and more, a portion of every political and military conflict takes place on the Internet, whose ubiquitous and unpredictable characteristics mean that the battles fought there can be just as important, if not more so, than the events taking place on the ground. Cyber attacks in support of nationalist political agendas or military actions have moved from the realm of theoretical debate into the real world. To date, there has been no attribution of an attack to any military or government entity, although assumptions are that most of the actions undertaken by patriotic hackers (or "hacktivists") have had the tacit support of the governments of their countries of origin.

The growth of sophisticated, persistent cyber-based espionage efforts targeting the United States over the past decade, made possible by the evolution of stealthier tools and techniques, has irrevocably altered the landscape of information security. Even as new threat actors and new tools that exploit user trust relationships and the vulnerabilities of signature-based perimeter defenses continue to populate this landscape, Government and industry information security remains largely focused on outmoded defensive techniques. New information security approaches are critically needed to combat these attacks, a majority of which are easy to execute, hard to prevent, increasingly difficult to detect, and highly successful.

The computer network-based threats to the nation's critical infrastructure pose another serious threat to national security. Many computer attacks and exploits that are more than capable of targeting the Supervisory Control and Data Acquisition (or SCADA) systems used to control valves and switches at manufacturing plants, power generators, and refineries have been created. Many networks are not adequately protected against the most current computer network attacks. The protections in place at many infrastructure facilities present few obstacles to skilled individuals or groups of attackers. Hackers may be able to gain access and take control of, or even crash, the systems running our power, water, traffic control, and other critical infrastructure systems.

---

[37] Jeff Bliss, *China's Spying Overwhelms U.S. Counterintelligence*, *Bloomberg*, April 2, 2007. | Shane Harris, "China's Cyber-Militia," The National Journal, Saturday, May 31, 2008, available online at: http://www.nationaljournal.com/njmagazine/cs_20080531_6948.php

[38] National Counterintelligence Executives, *FY07 Annual Report to Congress on Foreign Economic Collection and Industrial Espionage* at 3

Historically, the United States has enjoyed the geographic protection of broad oceans, but, today, geography has only limited value as we assess our national vulnerabilities. The military notion of a "front" – a defined line of battle safely distant from our homes, schools and places of business – is as antiquated as the buggy whip.

Our national prosperity and way of life is facing a looming threat from information attack because we are almost completely dependent upon information technology for our security and for our capability to continuously interact with nations around the world. As a result, the "front" is now everywhere. Cyber-attacks occur daily and they are increasing in both number and frequency. The race to defend against these attacks constitutes the most critical military and economic imperative of this century. It requires the input of the private sector in this nation, along with a new private sector partnership with Government. Moreover, it requires the cooperation of many other nations, all working in tandem, to meet these threats head on.

ISA SOCIAL CONTRACT

Cyber crime knows no "natural" boundaries. In this domain, the real distinction must be between people who share our values and those who do not. Entities in countries that share the values of American society must be empowered to ensure their own cyber security through access to whatever knowledge the US government has. This is the only way to shore-up friendly nations and to isolate rogue nations."[39]

"A related problem involves Government regulations that limit the ability of foreign students who specialize in this area to work in the US on cyber security issues. When foreign students seek to pursue cyber security research, they are often denied admission because NIST sensitive technology restrictions prohibit foreign access. These restrictions further limit the availability of candidates with the ability to expand the technological boundaries for improving cyber security."[40]

Quotes from the Obama Administration Cyber Space Policy Review

"The Nation also needs a strategy for cyber security designed to shape the international environment and bring like-minded nations together on a host of issues, such as technical standards and acceptable legal norms regarding territorial jurisdiction, sovereign responsibility, and use of force. International norms are critical to establishing a secure and thriving digital infrastructure. In addition, differing national and regional laws and practices—such as laws concerning the investigation and prosecution of cyber crime; data preservation, protection, and privacy; and approaches for network defense and response to cyber attacks—present serious challenges to achieving a safe, secure, and resilient digital environment. Only

[39] Internet Security Alliance, *The Cyber Security Social Contract: Policy Recommendations for the Obama Administration and the 111th Congress* at 29
[40] Internet Security Alliance, *The Cyber Security Social Contract: Policy Recommendations for the Obama Administration and the 111th Congress* at 22

by working with international partners can the United States best address these challenges, enhance cyber security, and reap the full benefits of the digital age."[41]

"Government and industry leaders — both nationally and internationally — need to delineate roles and responsibilities, integrate capabilities, and take ownership of the problem to develop holistic solutions. Only through such partnerships will the United States be able to enhance cyber security and reap the full benefits of the digital revolution. The global challenge of securing cyberspace requires an increased effort in multilateral forums. This effort should seek—in continued collaboration with the private sector — to improve the security of interoperable networks through the development of global standards, expand the legal system's capacity to combat cyber crime, continue to develop and promote best practices, and maintain stable and effective Internet governance."[42]

"International norms are critical to establishing a secure and thriving digital infrastructure. The United States needs to develop a strategy designed to shape the international environment and bring like-minded nations together on a host of issues, including acceptable norms regarding territorial jurisdiction, sovereign responsibility, and use of force."[43]

"Working with the private sector, the Federal government should coordinate and expand international partnerships to address the full range of cyber security-related activities, policies, and opportunities associated with the information and communications infrastructure upon which U.S. businesses, government services, the U.S. military, and nations depend."[44]

"Near Term Action Plan **#7:** Develop U.S. Government positions for an international cyber security policy framework and strengthen our international partnerships to create initiatives that address the full range of activities, policies, and opportunities associated with cyber security." [45]

RECOMMENDATIONS FOR ENHACING THE INTERNATIONAL APPROACH TO CYBER SECURITY

Recommendation 1: Establish permanent, multi-national collaborative centers for information security operations management.

---

[41] Obama Administration, Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure at 3.
[42] Obama Administration, Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure at 16.
[43] Obama Administration, Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure at 20.
[44] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure* at 21
[45] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure* at Executive Summary vi

The establishment of collaborative information security centers, modeled on the NATO Cyber Center of Excellence in Estonia and comprised of experts from multiple nations who are co-located, would be one way to make significant progress toward providing a focal point for incident response, promoting international cooperation on specific technical standards for information security, and providing a forum through which to disseminate knowledge and training on the subject of cyber security.

The benefits of long-term collaboration in a fixed location, rather than coming together for annual or semi-annual conferences, or bilateral summits, are the opportunity for the establishment of relationships and the promotion of long-term projects. Multi-national partners who staff these centers would be able to bring specific knowledge of the information security environments in their respective countries, which would benefit all member nations. Information like this has the potential to enhance threat awareness and to increase analytic sophistication among all staff members. Permanent centers or organizations would also outlast the specific individuals on staff and they would provide for a continuity of operations that is impossible when holding occasional meetings for information exchange. This model may also aid in the creation of accurate points-of-contact lists, comprised of information security professionals or government officials, and these lists could be referenced during international cyber incidents to improve coordination of response.

As in the Estonian center, these international centers of excellence for cyber defense would provide a multi-national forum for the creation of cyber defense doctrine, concept development, awareness and training, research and development, analysis and lessons learned, and consultation for the international private sector.

The Forum for Incident Response and Security Teams (FIRST), an international information security group comprised of international security professionals around the world, is another natural engagement point for the US Government and its allies on the issue of cyber security. FIRST has a secure, world-wide information distribution system for alerts, vulnerability announcements, and the exchange of analysis. FIRST also has a strong international network of deep technical expertise, making it an important potential ally in the creation of public-private information security partnerships.

Recommendation 2: Use U.S. membership in existing regional and multi-national forums to advocate for the adoption of detailed standards for cooperation on international cyber crime investigations.

The call for international agreements on cyber crime law enforcement has been made repeatedly, but many of the obstacles to actual implementation of these agreements arise from attempts to work via new agreements that are too broad in scope and too light on specifics, and, in many cases, involve nations with whom the US has had no previous framework for this type of cooperation. Using existing international organizational frameworks, and working through relevant sub-committees in groups like NATO, the Asia-Pacific Economic Cooperation (APEC) forum, and the Organization of American States (OAS), the U.S. Government can attempt to establish limited-scope agreements for the cooperative investigation of specific categories of transnational cyber crime. These agreements should

not attempt to "cover the waterfront" on the issue by seeking to define cooperation for all categories of cyber crime because specificity and narrowness of scope are the keys to success at the early stages of these international cooperative frameworks.
The Asia Pacific Economic Cooperation (APEC) forum has 21 member nations around the Pacific Rim, including some of the largest economies in the world as well as nations with some of the most pressing cyber security issues in the world. An organization of this stature, scope, and resources could be a powerful framework from which to create additional cyber security centers of excellence or through which to establish a framework for cyber crime law enforcement. APEC's existing Telecommunications and Information Working Group (TEL) is a potential starting point for the creation of these centers. The TEL aims to improve telecommunications and information infrastructure in the Asia-Pacific region through the development and implementation of appropriate telecommunications and information policies.

The TEL has already published the *APEC Cyber Security Strategy*, which successfully codified mutually acceptable norms for cyber security. The US should recognize this framework as the point of departure for the development of specific cyber crime law enforcement initiatives and/or agreements. Already, the United Nations has acknowledged the importance of securing international communications infrastructure (UNGA Resolution 55/63) as has the Organization for Economic Cooperation and Development (OECD's Network Security Guidelines).

Similar international economic, political, and trade organizations, such as the Association of Southeast Asian Nations (ASEAN), the G-20, or smaller, sector-specific, regional groups such as the African Information Security Association, all represent potential avenues for U.S. Government and for private sector entities to propose this type of collaboration and information sharing in a common location.

A FRAMEWORK FOR SECURING THE GLOBAL "IT" SUPPLY CHAIN

The Internet Security Alliance, in collaboration with Carnegie Mellon University, has been working on Supply Chain issues for over two years. Two major conferences were involved, and over one hundred experts from industry, government, and academia contributed to this effort, which resulted in an initial report by Carnegie Mellon staff. Subsequently, ISA has continued this work in conjunction with Scott Borg, Director of the U.S. Cyber Consequences Unit, who developed the present framework.

THE PROBLEM

There is a serious danger in the fact that the supply chain for electronic components, including microchips, could be infiltrated by hostile agents at some stage of the chain. These hostile agents could alter the circuitry of the electronic components or they could substitute counterfeit components with altered circuitry. The altered circuitry could contain "malicious firmware" that would function in much the same way as malicious software. If the electronic components were ever connected to a network that the enemy attackers could access, the malicious firmware could give the attackers control of the targeted information systems.

Even if the malicious firmware was not connected to a network accessible to the attackers, the firmware could still contain logic bombs that could cause terrible harm. A logic bomb in a weapons system, for example, could lie dormant until the system engaged in certain activities that indicate a high degree of mobilization. These symptoms of mobilization could then trigger the logic bomb. The logic bomb could shut down the larger information system or, worse, turn the equipment controlled by the information system against those operating the equipment.

Once malicious firmware has been inserted into electronic components, it can be almost impossible to detect. The malware will remain in place if or when all of the software is upgraded or replaced. The circuits in which the malware could be hidden are microscopically small and enormously complex. What's more, like malicious software, it is possible to look directly at malicious firmware and not see anything wrong with it. Cleverly written malware will perform the kinds of operations that an information system is routinely supposed to perform - it will just perform those operations at exactly the wrong time.

THE ISA SOCIAL CONTRACT ON SUPPLY CHAIN

The government's *Cyberspace Policy Review* not only recognizes the extent of the problem, but also the need for a balanced approach to solving the problem:

"Government needs to be involved in supply chain issues and support solutions that are economically practical for the private sector. This would include working with the private

sector to develop a consensus framework to assure secure systems. This needs to be done on an international basis with market motivators that transcend national boundaries."[46]

"The supply chain issues also create obstacles. We need to test and screen equipment we get from our vendors. This means we need to have a secure and trusted relationship with these vendors and that they are following through properly. There also needs to be appropriate training especially for people involved in these issues overseas. For organizations that have not yet made cyber security a true priority there are other barriers, often primarily economic."[47]

"However, the emergence of new centers for manufacturing, design, and research across the globe raises concerns about the potential for easier subversion of computers and networks through subtle hardware or software manipulations.
A broad, holistic approach to risk management is required rather than a wholesale condemnation of foreign products and services. The challenge with supply chain attacks is that a sophisticated adversary might narrowly focus on particular systems and make manipulation virtually impossible to discover. Foreign manufacturing does present easier opportunities for nation-state adversaries to subvert products; however, the same goals could be achieved in domestic manufacturing through the recruitment of key insiders or other espionage activities.
The best defense may be to ensure U.S. market leadership through continued innovation that enhances U.S. market leadership and the application of best practices in maintaining diverse, resilient supply chains and infrastructures."[48]

ISSUES THAT NEED TO BE ADDRESSED TO MOVE FORWARD

The *Cyberspace Policy Review* recommends a holistic approach to risk management that is practical from both an operational and a business support model. The risk of inserting malware/spyware insertion is greater in some foreign countries simply because, in some cases, the governments in those countries provide support for this type of activity and, also, have ample resources - including the ability to intervene in the manufacturing processes using regulations- to do so. However, given sufficient resources, simpler attacks like this could happen domestically.

The Administration's review is correct in that there is a preference for doing the detailed work of the supply chain overseas, and that's where the back-door potential is highest. For example, a PC could have final assembly in the U.S., but the network chip, disk drive, and firmware would come from other countries. It would be much harder to detect and stop

---

[46] Internet Security Alliance, *The Cyber Security Social Contract: Policy Recommendations for the Obama Administration and the 111th Congress* at 17
[47] Internet Security Alliance, *The Cyber Security Social Contract: Policy Recommendations for the Obama Administration and the 111th Congress* at 15
[48] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure* at 34

malware during the manufacture of those components than it would be to stop someone from inserting something in the PC case during final assembly in this country.

Among the issues that need to be addressed are the following:

First, there are those things that result in the corruption of, or lack of trust in, the final product. This includes the deliberate subversion or accidental corruption of hardware, firmware, or software. This type of alteration is very difficult to detect at later manufacturing stages. Assurance and inspection processes need to be in place at the appropriate manufacturing stages to detect any such corruption or subversion of the product or its components.

Second, the different enterprises engaged in a collaborative project need a secure method through which to communicate and collaborate that supports the necessary trust relationships. This approach generally takes the form of some type of federated identity, authenticated to a specific trust level and is used to gain access to resources that have been authorized by the cooperating parties. Controls need to be in place so that an attacker cannot leverage these relationships to spread attacks among collaborating enterprises.

Finally, enterprises need a way to ensure that the necessary governance protections are in place as part of their formal agreements. This should include establishing a contract of policies, security procedures, rules governing the disclosure of breaches, auditing and evidence gathering procedures, as well as other related processes. Standard definitions and operating levels are necessary among the engaged parties in order to assess the risk at each manufacturing stage and to provide appropriate legal and technical countermeasures.

To address these issues, ISA proposes the following framework for a holistic risk management supply chain program which addresses the technical, legal, and economic issues as suggested in both the ISA Social Contract and the Obama Cyber Space Policy Review.

THE ECONOMIC OBSTACLES

To prevent malicious firmware from getting into government, military, and critical infrastructure systems, a number of government officials have previously proposed severe counter-measures. These counter-measures would require that the design, fabrication, assembly, and distribution of the electronic components destined for government systems to be carried out domestically, in strictly controlled facilities, under constant and close supervision by carefully vetted personnel, and with numerous verification procedures. The idea would be to institute these counter-measures through government mandates and as provisions in government contracts.

The problem, however, is that this sort of security program would not be economically viable. The costs of supplying electronic components in this way would be much greater than the government would be willing, or able, to pay. If the government suddenly demanded stringent supply chain security of this kind, the companies involved in the chain would simply

stop supplying the government. Electronic manufacturers that also supply broad, non-government markets could walk away from their government business quite easily. As a result, the few specialty manufacturers that only supply the government would be put in an impossible economic situation and would simply go out of business.

There are no regulatory policies that could easily change the response of the electronics industry to government demands for strict supply chain security. The high costs of imposing such security are partly due to the multi-national nature of electronics production. This multi-national production is competitively necessary. Imposing costly requirements on American companies would limit their ability to compete internationally. Protecting less competitive operations through public subsidies is not a sustainable national policy. Over time, subsidies, whether they take the form of tariffs or price supports, tend to make the subsidized industries less and less competitive. In the electronics industry, where international competition drives rapidly falling costs, this would be especially true.

Where electronic components are concerned, the conflict between economic requirements and security requirements seems insurmountable.

BEING REALISTIC ABOUT THE ADVERSARIES

Despite the seriousness of the problem, it is important to keep it in perspective because, actually, there are limited motives and limited targets for malicious firmware. It is very expensive and very time-consuming to infiltrate a supply chain deeply enough to insert malicious firmware. Also, after the firmware was employed in a cyber attack, it would be difficult to employ it again. Anyone profiting from a supply chain would be reluctant to insert firmware that would discredit that supply chain and the losses would simply be too great. While many attackers could achieve their ends by utilizing malicious firmware, nearly all of the attackers could achieve the same ends more cheaply and more quickly by employing malicious software.

However, attackers who would be seriously interested in malicious firmware would be nation-states. Nation-states would be interested in installing sleeper, one-use attack tools, because part of a nation-state's mission is to prepare defensive tools that would only be used in an extreme circumstance. They are willing to put up with very long preparation times if they can obtain capabilities that are long lasting. They are very interested in targeting hard-to access systems, such as highly protected military, intelligence, and infrastructure facilities. They are happy to invest in dormant capabilities that would sit for long periods without any interaction or operation. Finally, when larger security issues were at stake, nation-states would be willing to sacrifice the profits they might otherwise make via their participation in global supply chains.

There are also certain circumstances in which large criminal conspiracies would be interested in utilizing malicious firmware. These are cases where the criminals could obtain large profits through the corruption of electronic equipment that has no software to corrupt. One example of this type of equipment is credit card readers, which were recently corrupted in the

supply chain, thereby allowing thieves to steal tens of millions Euros by hijacking information from European retail transactions. Another example of this type of equipment is automated security systems, through which criminals who have tampered with supply chains can gain physical access to otherwise secure facilities.

Apart from nation-states and very specialized criminal conspiracies, there are very few attackers who would be interested in employing malicious firmware. Therefore, although malicious firmware is a very severe and important problem, it is nonetheless a very limited problem.

THE STRATEGY

What, then, is to be done about this? The ISA's answer is to solve the problem of malicious firmware in a way that produces other security benefits at the same time. That way, these other benefits can justify the security expenditures necessary to combat malicious firmware.

In a similar manner, the use of technologies such as identity federation and strong credentials can not only increase the security of the virtual relationships between supply chain members, but also provide the assurance for closer collaboration and the elimination of duplicate security processes, resulting in more efficient operations.

Standards such as the ISO 27000 series and the NIST 800 documents provide a neutral way for supply chain members to evaluate each other's security maturity and to manage their risks accordingly

While businesses are not currently suffering significant losses from malicious firmware, they are constantly suffering *other* losses from security problems in their global supply chains. Many of these other losses are already large and they threaten to become much larger. Businesses are regularly threatened with interruptions in their own supply chains that cause production delays and greatly increase their costs. Businesses are threatened with quality control problems among their suppliers that can greatly damage their brands. Businesses face problems with counterfeit products that cause a reduction in sales, along with further damage to the business' brand when the counterfeit products prove defective. Moreover, and perhaps most importantly, businesses are threatened with losses of intellectual properties that could, ultimately, undermine their future ability to compete.

The key to solving the problem of malicious firmware is to make the entire global supply chain more secure so that it can cope with these other threats, as well. Therefore, any measures taken to protect against malicious firmware must be part of a more comprehensive security program. The emphasis on a more comprehensive approach also makes sense in more basic ways - security measures are by nature complementary and need to be applied together in order to be effective.

THE FRAMEWORK

From a business standpoint, there are four kinds of cyber attacks that are possible at each stage of the supply chain (Borg Categories):

1) Cyber attackers could interrupt the operation.
2) Cyber attackers could corrupt the operation (including inserting malware).
3) Cyber attackers could discredit the operation (undermining trust, damaging brand value).
4) Cyber attackers could undermine the basis for the operation (loss of control, loss of competitively important information).

For each of these different kinds of cyber attacks, there are different remedies, some of which can be identified by brief bullet points.

1) Protection against interruption:
    - Continual, mandatory sharing of production across supply chain.
    - Maintaining alternative sources.
2) Protection against insertion of malware:
    - Strict control of environments where key intellectual property is being applied.
    - Logical tamper-revealing seals (hash functions, feature checks).
    - Physical tamper-revealing seals (e.g. container seals).
    - Effective sealing and tracking of containers.
3) Protection against undermining trust:
    - Logging of every operation and who is responsible for that operation.
    - Bonded operators and facilities.
4) Protection against loss of control of information:
    - Versioning as a tool for protecting intellectual properties.

There are five different supply chain stages to which the remedies need to be applied:

I. The Design Phase.
II. The Fabrication Phase.
III. The Assembly Phase.
IV. The Distribution Phase.
V. The Maintenance Phase.

Each of these phases can be further divided into the basic sequences of operations that need to be carried out during that specific phase. The Design Phase, for example, can be divided into the overall product design (which divides further into the specification of electronic inputs and outputs and the specification of overall physical design features), the detailed product design (which divides into the schematic diagrams created using circuit design software, the physical circuit layouts created using circuit layout software, and the physical assembly, engineering and design), and the creation of production masters (which divide into wafer mask production and the creation of prototypes, templates, and molds). These generic divisions are remarkably uniform for different electronic components.

If we combine the list of remedies with the stages of the supply chain to which they need to be applied, we get a "Remedies for Stages Grid."

	REMEDIES				
STAGES		1) Protections against the *interruption* of production	2) Protections against the *corruption* of production	3) Protections against the *discrediting* of production	4) Protections against the *loss of control* of production
	I. Design Phase				
	II. Fabrication Phase				
	III. Assembly Phase				
	IV. Distribution Phase				
	V. Maintenance Phase				

This framework should provide a systematic way of both identifying and applying the relevant security measures to the electronics supply chain. It should also be helpful in identifying the areas where new security techniques need to be developed.

COLLABORATION ISSUES

Common to all stages in the framework are the risks of collaboration. While these risks may increase as more and different types of electronic communication are employed, there are specific steps that can be taken to reduce these collaborative risks. Some examples are:

1) The use of hardware-based credentials, such as smart cards, instead of passwords to present digital identities of supply chain members will limit the ability of an attacker to traverse the supply chain with forged identities.
2) The use of health checking protocols (IETF NEA, TCG IF-MAP looking at patch levels, AV status) will reduce the risk of supply chain members transmitting malware when contacting each other' services.
3) The use of encryption or other access control protections when exchanging information will help to protect information, making it harder for an adversary to steal the information or to corrupt it in a manner similar to the aforementioned firmware risks.

Security technologies such as identity federation and strong credentials can increase the security of the virtual relationships between supply chain members, and they can also provide

the assurance for closer collaboration and the elimination of duplicate security processes, resulting in more efficient operations.

THE LEGAL SUPPORT

In order for this security framework to be instituted effectively, certain legal relationships are necessary between the global component suppliers, the assemblers, and the company overseeing production.

1) There need to be rigorous, unambiguous contracts, which delineate the security measures.
2) There need to be locally responsible corporations with a long-term interest in complying with these contracts.
3) There need to be local methods of overcoming agency problems and for motivating executives and workers.
4) There needs to be adequate provision for verifying the proper implementation of security measures.
5) There needs to be local enforcement of agreements at all levels.

The legal incentives created by these measures do not need to be strong enough to deter the infiltration of the supply chain by potential attackers. They simply need to be strong enough to motivate widespread compliance with the relevant monitoring procedures. If the monitoring procedures are well designed, they will normally provide adequate warning of breakdowns in the security procedures.

ISA'S MODEL FOR MEETING THE GOVERNMENT'S NEEDS

After the framework for securing the electronics supply chain has been established, after the specific techniques have been developed, and after the legal support is in place, it may still be necessary for the government to pay a premium for the high degree of security it needs for critical systems. But, by this point, the premium that is needed should be a relatively modest one. The measures necessary for reducing the risk from malicious firmware will be part of a broader program that is being widely applied to secure all of the key aspects of the electronic supply chain.

NAVIGATING LEGAL COMPLIANCE & SECURITY WHEN USING DIGITAL COMMUNICATIONS

LEGAL STRUCTURES ARE RACING TO KEEP UP WITH DIGITAL TECHNOLOGY

In many countries, including the United States, courts are struggling to adapt older laws and legal principles to the challenges created by the tremendous capabilities of computing net working and mobile devices, and the rising economic significance of digital information as a class of property to be created, bought, sold, stolen, and destroyed. Unified Communications (UC) products (e.g., VoIP and IM) and services potentially collide against many different laws and regulations, and this is, according to both the Internet Security Alliance and the Obama Administration, an area in need of urgent attention.

While it is beyond the scope of the ISA alone to resolve this problem, at the request of its members, the ISA created a handbook to provide assistance in navigating the convergence, or lack thereof, of technology and law. Recently, the ISA decided to make this handbook available to the general public free of charge. The document is available for free download at ISA's web site (www.isalliance.org), and hard copies of the document can be purchased for a nominal printing charge by contacting the ISA directly.

ISAlliance Stated Position

Despite the enormous economic and competitive potential of unified communications technologies (e.g., voip, IM etc.), genuine and serious issues exist as to whether 20th century laws prevent corporations from employing conventional and effective Internet security practices to protect their networks, computers, data and business partners against malicious and criminal misconduct. As a result, because of this inability to apply security controls:

- Corporations are withholding their investments in UC solutions; doing so inhibits the corporations' ability to access increased operational efficiencies offered by UC technologies.
- Businesses are limiting their use of UC solutions in order to disallow any Internet activity against which existing, effective security controls can be employed. This practice limits the availability and use of various third party services, and, thereby, also increases the implementation costs (as a general matter, internally installed UC solutions are more expensive than Internet-based solutions provided by third parties).
- Business networks — customers, suppliers and service providers creating communities and markets through the Internet are handicapped from integrating UC solutions into their operations because of the inability to secure the Internet-related traffic.

In addition, regulations and interpretations of existing laws that were proposed during the final months of the Bush administration suggested that, since UC solutions empower normal companies with the ability to provide the same services as Internet telephony, any company operating UC-related servers and routers would be considered as a "communication common carrier", subject to both the investigative and the warrant powers of the Federal government

(as well as to minimum technology standards that enable expedited access and monitoring by Federal authorities of the related communications). The specter of the potential imposition of Federal investigatory powers on any company offering UC solutions, even for internal use only, has further handicapped the appeal of these new technologies.

It is inconsistent with new Federal policy to stimulate the economy to allow 20th century computer laws — and the risks of prosecution or unacceptable intrusion into corporate networks — to inhibit the availability of new technology solutions that enable American companies to realize new efficiencies and competitive advantages. Applying sound, conventional security controls to any Internet-based packet traffic should not be the basis for potential Federal legal action. Instead, the legal framework must be reviewed and revised, so that strong, consistent corporate security practices can be employed. The end point should not be an abandonment of the important policy interests served by ECPA, CALEA, and other 20th century laws; instead, a different balance is required, one that enables public-private sector partnerships to expand and mature so that security activities may properly focus on the truly bad actors who threaten the integrity and operations of American networks and who challenge our collective cyber security investments.

Quotes from the Obama Administration Cyber Space Policy Review

"Scores of legal issues emerged, such as considerations related to the aggregation of authorities, what authorities are available for the government to protect privately owned critical infrastructure, the placement of Internet monitoring software, the use of automated attack detection and warning sensors, data sharing with third parties within the Federal government, and liability protections for the private sector."[49]

"The review team found that throughout the evolution of the information and communications infrastructure, missions and authorities were vested with various departments and agencies by laws and policies enacted to govern aspects of what were then very diverse and discrete technologies and industries. The programs that evolved from those missions were focused on the particular issue or technology of the day and were not necessarily considered with the broad perspective needed to match today's sweeping digital dependence."[50]

"As traditional telecommunications and Internet-type networks continue to converge and other infrastructure sectors adopt the Internet as a primary means of interconnectivity, law and policy should continue to seek an integrated approach that combines the benefits of flexibility and diversity of applications and services with the protection of civil liberties, privacy rights, public safety, and national and economic security interests. A paucity of judicial opinions in several areas poses both opportunities and risks that policy makers should appreciate—courts can intervene to shape the application of law, particularly in areas involving Constitutional

[49] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure* at 3.

[50] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure* at 3.

rights. Policy decisions will necessarily be shaped and bounded by the legal framework in which they are made, and policy consideration may help identify gaps and challenges in current laws and inform necessary developments in the law. That process may prompt proposals for a new legislative framework to rationalize the patchwork of overlapping laws that apply to information, telecommunications, networks, and technologies, or the application of new interpretations of existing laws in ways to meet technological evolution and policy goals, consistent with U.S. Constitutional principles. However, pursuing either course risks outcomes that may make certain activities conducted by the Federal government to protect information and communications infrastructure more difficult."[51]

OUTLINE OF ISA HANDBOOK ON UNIFIED COMMUNICTIONS

In 2008, the Internet Security Alliance Board of Directors authorized a project to evaluate whether legal concerns may be restraining companies (or service providers) from fully deploying conventional Internet security services with respect to VoIP and other unified communication services and, if so, to develop recommendations on how those legal concerns may be addressed.

Report Scope and Objectives

The Report is intended to be a pragmatic, useful resource for companies that are both suppliers and customers of unified communication services, with a special focus on meeting the needs of in-house legal counsel that have been asked to evaluate the legal suitability of employing unified communications in their business. As such, the Report describes the existing technologies of unified communications (UC) and, in particular, the relevant technical aspects that are useful to understand in conducting a legal analysis.

The Report provides an overview of how UC solutions confront Internet security risks and highlights some of the essential Internet security services that can be used to protect a company, its facilities, its properties (including business data) and its employees and agents. Further, the Report provides an inventory of the relevant laws to be considered in launching and operating unified communications products and services (from the customer's perspective), emphasizing U.S. laws, notably the Electronic Communication Act.

Despite its limitations, the Report is believed to be the most detailed analysis to date of the applicability of current federal law to the use of Internet security services to protect UC solutions and services and, therefore, substantially advances toward the original objectives of the Privacy Act and the Stored Communications Act (collectively referred to as ECPA). The Report's inventory presents a detailed analysis of ECPA and its terms. It delivers a detailed analysis that enables lawyers and their clients to evaluate whether ECPA creates legal barriers to the corporate use of relevant Internet security services in connection with UC products and services. Also, the Report includes a practice toolkit of recommended practices and checklists for lawyers and their

[51] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure* at 10.

clients to better assure that the use of UC solutions and services does not produce unexpected legal exposure or risk. Further, the Report presents a Glossary and a Legal and IT Resource Inventory, providing bibliographic references to the key legal and technology resources we consulted in preparing the Report. The reliance on those resources, as well as additional comments on the research, is outlined at the end of the report.

CREATING STANDARDS TO AUTOMATE SECURITY IN THE VoIP PLATFORM

THE PROMISE AND PROBLEMS OF UNIFIED DIGITAL MEDIA PLATFORMS

From Navigating Compliance and Security for Unified Communications

Technology innovations often defy the boundaries imposed by precise definitions. Unified communications (UC), when viewed as a single portfolio of solutions, deliver exciting and compelling functionality and enormous business value.

Unified communications offer a cornucopia of solutions that are blurring the distinctions between audio, video, and data networks. Some view the emergence of UC as a development as profound as the Internet itself. UC solutions facilitate the integration of corporate networks, business communities, and market systems, thereby eliminating the need for separate network structures (such as phone systems, cell phone systems, data networks, video networks) that require extensive technical support to enable content migration.

UC solutions offer, and deliver, a compelling business case for improving the efficiency and p roductivity of every connected enterprise resource: computers, devices, networks, data and pe ople. By employing technology to connect and unify the availability of communication conten t, the solutions overcome persistent issues in business that have persistently blocked organizat ions from realizing the full potential of existing technology to improve the agility, responsive ness and effectiveness of the enterprise. UC solutions address:

- *Time delays caused by personnel travel, mobility and inaccessibility*
- *Accuracy and time delays caused by manually converting or transferring content between media.*
- *Inability to prioritize access or availability.*

In delivering those benefits, UC solutions directly draw into question the continued investmen t in, and operation of, more traditional business media.

Those costs can be substantial, both in terms of direct expenses incurred for third party services and support, as well as the internal resources assigned to acquire and operate internal phone networks and to provide administrative support (e.g., calculation of charges, equipment management and replacement, etc.). For many companies, eliminating these costs and migrating all of the company's communication activities onto an Internet based UC platform offers a compelling proposition, particularly in economically challenging times.

The proliferation of hyper-connected IP devices in the enterprise, the need to be able to ensure that these devices introduce no known vulnerabilities, are properly patched, and are securely configured is critical, especially so in terms of enterprise voice services. The ability to do these things automatically on a periodic basis will improve the overall assurance of the organization's voice solution, and will provide an increase in security posture of voice services.

IP enabled devices ranging from Blue-ray players, copiers, heating and cooling systems, phones, thermostats, coffee makers, and refrigerators have entered the marketplace for both business and residential users. Ensuring that this eclectic collection of devices - as well as the more traditional routers, switches, laptops/desktops, servers, and printers - have the most up-to-date patches, present no known security vulnerabilities, and are configured to represent the organization's security policy, is a growing challenge for the people responsible for the cyber security of these networks.

However, while the business economics, especially in a world economy, literally demand the use of increasingly efficient digital media, these platforms come with daunting security implications, implications clearly recognized in the Obama Cyber Space Policy Review.

From the Cyber Space Policy Review

"The digital infrastructure's architecture was driven more by considerations of interoperability and efficiency than of security. Consequently, a growing array of state and non-state actors are compromising, stealing, changing, or destroying information, and these actors could cause critical disruptions to U.S. systems. At the same time, traditional telecommunications and Internet networks continue to converge, and other infrastructure sectors are adopting the Internet as a primary means of interconnectivity. The United States faces the dual challenge of maintaining an environment that promotes efficiency, innovation, economic prosperity, and free trade while also promoting safety, security, civil liberties, and privacy rights."[52]

"The thirteen years since the Telecommunications Act was passed have witnessed significant growth and transformation in the telecommunications marketplace. Advanced wireline and, increasingly, wireless broadband network infrastructures have been (and continue to be) deployed that provide an increasingly diverse array of applications and services to both commercial and individual users, accessible over a growing variety of fixed and mobile devices. They support the clearing of billions of dollars in transactions among financial institutions, trading on exchanges, online banking, e-commerce, as well as billing and account management for many retailers and service providers; they facilitate rapid, global communications and the storage and transfer of enormous volumes of information, including proprietary business information, intellectual property, customer account and transaction information, and other personally identifiable private user information such as health records; they make an array of heretofore inaccessible information available at the user's fingertips

[52] Obama Administration, Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure at iii

with a few keystrokes. They have also become essential elements in the operation and management of a range of critical infrastructure functions, including transportation systems, shipping, the electric power grid, oil and gas pipelines, nuclear plants, water systems, critical manufacturing, and many others."[53]

"As dependence on these converged systems grew, users and network managers became aware of new types of vulnerabilities in the infrastructure. Moreover, the rapid emergence of the online commercial environment, the growing monetary value of transactions, and the increasing volume of sensitive information accessible online have also increased the online threat landscape by fueling the growth of organized criminal elements and other adversaries. Not only was it necessary to protect the information content, it became necessary to ensure the confidentiality of information as well as the authenticity of its sender and recipient."[54]

"Effectively addressing the fragmentary and diverse nature of the technical, economic, legal, and policy challenges will require a leadership and coordination framework that can stitch this patchwork together into an integrated whole."[55]

As the Director of National Intelligence (DNI) recently stated in testimony before Congress, the growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructures. The Intelligence Community assesses that a number of nations already have the technical capability to conduct such attacks.[56]

ISA/NIST PROJECT TO CREATE AUTOMATED CYBER SECURITY FOR VOIP

In March 2008, the Internet Security Alliance Board of Directors authorized a project, in cooperation with the National Institute of Standards and Technology (NIST), to develop a set of technical materials for improving the security available for Voice over Internet Protocol (VoIP) services. The ISA Board recognized that the economics of the modern economy made almost inevitable the prospect of an ever-increasing use of multiple digital converged platforms, while, simultaneously, multiplying the range of security issues due to the rapid increase in devices that were being used for converged purposes.

As a result, the most practical solution would be to try to devise an automated system to address security issues that would be offered on an open source basis and would secure the entire platform. The most logical starting point would be the production of a

[53] Obama Administration, Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure at c-9.
[54] Obama Administration, Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure at c-10.
[55] Obama Administration, Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure at c-12.
[56] Obama Administration, Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure at 1-2

Security Content Automation Protocol (or SCAP) to enable automated vulnerability management, measurement, and policy compliance for VoIP services. Immediately a question was raised: **would SCAP help to address the issues identified with enterprise VoIP deployments?**

SCAP is a recommended approach for U.S. Federal Government Organizations to demonstrate compliance with security requirements in mandates such as the Federal Information Security management Act. SCAP may be viewed as being comprised of two distinct elements. First, and foremost, SCAP is considered a protocol that is comprised of specifications (currently two XML languages, three enumeration standards, and one scoring/metric standard) that standardize how one assesses and communicates information about software flaws and security configurations. Secondly, content developed in the SCAP protocol may be viewed as providing software vulnerabilities and security configuration reference data. Today, this content is available from public repositories such as the National Vulnerability Database (NVD), from software publishers such as Redhat, and, often, from security tool vendors that provide NIST SCAP Validated tools.

SCAP can be used for security configuration verification, requirements traceability, standardized security enumerations, and vulnerability measurement. From an enterprise voice perspective, SCAP addresses three critical areas in providing a solutions level of assurance: the management of security vulnerabilities, the management of corrective content (patches), and the management of security configuration.

The initial use case that encouraged wide-spread adoption of SCAP is the recent mandate for secure desktop configuration known as the Federal Desktop Core Configuration (FDCC). FDCC required the entire federal government to harden their Microsoft Windows XP and VISTA desktops in accordance with the minimum security settings represented by the mandate. This presented a significant challenge, in that proprietary configuration assessment tools provide proprietary results assessments. Given a government-wide mandate for this configuration, the desire to have a common, open, public domain method of assessing and reporting these configurations became paramount, and additional guidance has been published by the Office of Management and Budget (OMB) requiring use of SCAP Validated tools for several tasks, including continuous monitoring of the FDCC control settings.

But SCAP has never been limited to desktop assessments; the FDCC just represented the most visible initial use case. SCAP can be applied more broadly to practically any device and operating system, and there are numerous use cases that continue to be developed by vendors, as well as by public and private sector organizations. SCAP may also be leveraged in parts. For example, some vendors publish Threat Advisories that may include SCAP enumerations and metrics, but may not include the SCAP XML system checks. SCAP may also be leveraged with all components on different platforms such as servers, network devices, et al. As a relatively new standard, SCAP also has several emerging specifications that are being evaluated for potential inclusion in the protocol (at some future date), based on industry and government requirements and feedback.

The ISA reached out to contacts within NIST and DHS to solicit their reaction to an ISA-led program to assess the applicability of the SCAP program to enterprise VoIP solutions, and to develop appropriate SCAP content. NIST and DHS were extremely supportive of the proposal and they encouraged the ISA to continue with the incubation of its idea.

In September 2008, the ISA presented their VoIP SCAP proposal to the Information Security Automation Conference in Gaithersburg, MD, during a daylong workshop. This was followed up by a year-long project in which nearly 60 corporations and government agencies attempted to assess the applicability of the SCAP approach to real-time systems, such as enterprise VoIP solutions, and how to develop reference SCAP content to establish a minimum baseline for appropriate VoIP configurations.

In October 2009, ISA led three sessions at the NIST Information Security Automation conference in Baltimore in which it presented the results of its work to date.

In 2010, the ISA will continue the VoIP project through broader outreach to the community and by expanding their view beyond SCAP to other potential automated solutions.

APPENDIX A

Federal investment in our collective cyber-security posture will be most effective by adopting a broad set of incentives that serve to:

- ◊ increase the benefits of "doing right,"
- ◊ decrease the costs of "doing right."
- ◊ decrease the benefits of "doing wrong."
- ◊ increase social stigma of "doing wrong"

Differing objectives will call for different incentive measures. For example, concerns over entities that practice poor cyber-citizenship may pose a threat to others via their susceptibility to bot-nets. Today, the consequences to others borne by an entities poor cyber-citizenship are not recognized by the perpetrator. An effective incentive model would call for internalizing today's externalities, by denying tax-breaks and the incentives that may be offered to others who do harden their systems against bot-net take-overs. Alternatively, those entities who do incorporate the practices of good cyber-citizenship may be rewarded with tax-breaks and subsidies that encourage investment and implementation of cyber-security technologies and best practices. The diagram below depicts desired behaviors of good cyber-citizenship in the arrows. Overarching classes of incentive response are noted in the four grids, while example incentive responses supported by the Government are highlighted within the grid.

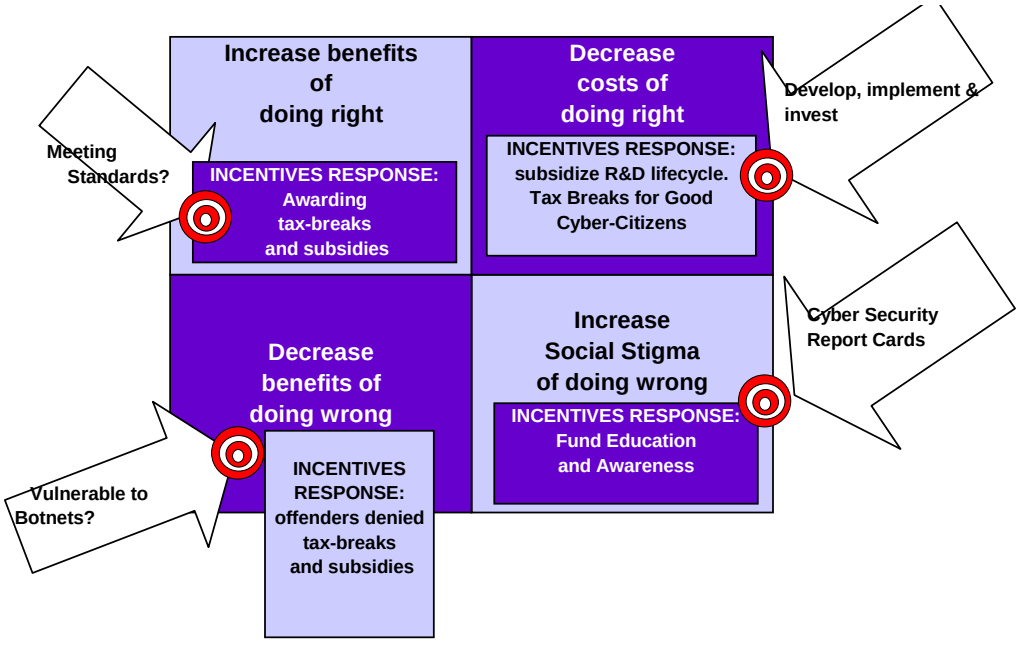

Figure 1: Matrix of Incentive Solutions and Cyber Citizenship Goals

It should also be noted that incentives should be structured in a manner consistent with the importance and possible risks posed to the nation by serious cyber-security breaches. Utilizing the eighteen named Critical Infrastructure Key Resources (CIKR) as established by the Patriot Act as a prioritizing and filtering mechanism for the implementation of incentives

allows the Government to leverage much work in this regard already performed by the Department of Homeland Security.

Specifically, the incentives structures would follow a tiered implementation so that those entities whose functions were central and core to an identified CIKR would have the highest expectations with regard to their standards of cyber citizenship, and be subject to the highest rewards, and highest disincentives. Two additional tiers of entities, differentiated by scale, volume and scope would be subject to the incentives established, but with lesser rewards and penalties. Such a split across CIKR core, first and second tier entities is depicted in Figure 2.

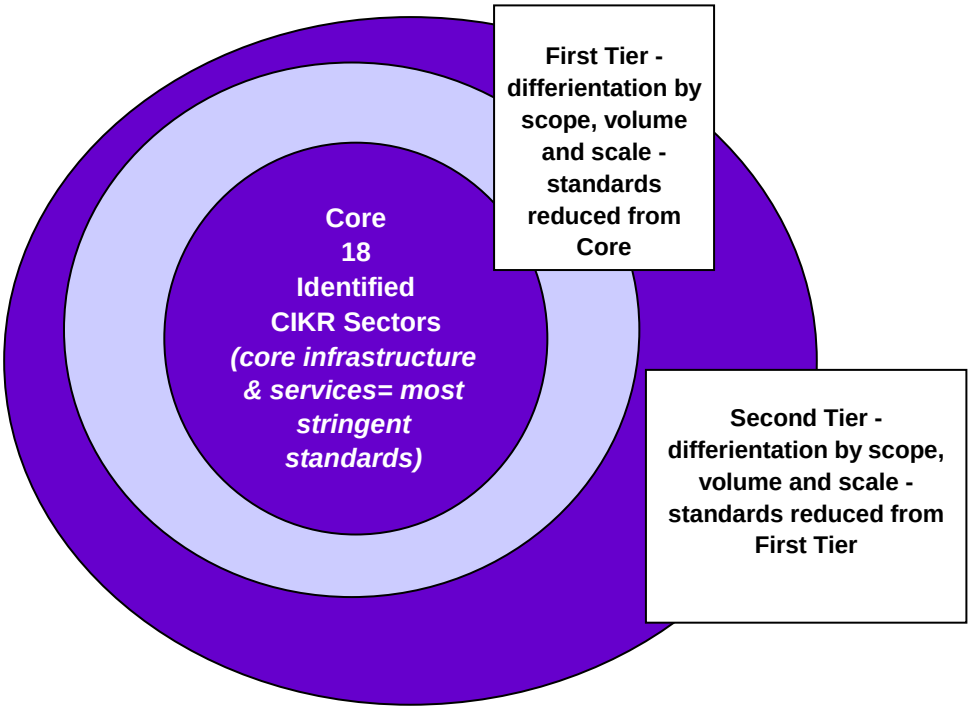

Figure 2: Core CIKR Sectors, with First and Second Tier Entities

APPENDIX B

THE SOCIAL CONTRACT FOR CRITICAL INFRASTRUCTURE

Widespread use of the Internet in Critical Infrastructure may create new vulnerabilities in real-time control and incident response that undermine improvements in service and cost. Industry may not prioritize its Internet security development agenda around these issues. Who will?

Critical Infrastructure (CI) systems, from refineries and energy transmission systems, to railroad control and securities trading systems, are highly complex systems of systems. As CI systems increase their dependence upon cyber technology, particularly the Internet, they become vulnerable to new threats with multiple and severe consequences of national scale. System breaches or vulnerability exploitations of these so-called "cyber-physical" systems may compromise public safety, industry/economic vitality, individual and enterprise privacy, and continuity of operations for vital government institutions, and special care must be taken to contain their impact. Some vulnerability exploitations can be prevented, or their consequences mitigated, with emerging cyber security technology. Some vulnerabilities can not, however, be prevented, particularly where a breach of real-time control causes significant, immediate, and irreversible damage.

WHAT'S AT STAKE?

Many issues trade off the balance between cost/service improvements and safeguards that minimize and mitigate new vulnerabilities and their consequences. Among these issues that collectively impact national security, economic vitality and public confidence are:

- Service availability and stability
- Public safety
- Enterprise and public information privacy
- Emergency response and disaster recovery, and
- Continuity of operation of key Government Institutions.

WHY IS THE SOCIAL CONTRACT REQUIRED NOW?

Internet security has not yet progressed to the point where it can prevent or detect all breaches and exploitations that affect critical control signals in real-time. The continual leap-frog activity of seeing new attacks and then developing protections to reduce future occurrence or impact is sufficient for many traditional IT applications, but not for potentially volatile control or emergency response systems, where service availability must be absolute at the time of an incident. Until Internet security achieves the ability to preemptively prevent certain attacks and achieve complete detection and attribution, there remain certain functions of CIP that should be designed around, not into, an Internet-centric architecture. Industry will develop near-sufficient internet security (promoting it as the state of the art) - filling the void with solutions that may be short of the national need. New commercial products and services will strengthen the Internet only to the extent that fits the budgets, priorities, and time-to-market plans dictated by competitive market conditions, thus establishing a baseline unsuitable to completely protect the national interests in CI - but establishing the new status quo, nonetheless.

The Social Contract is required at the beginning of this new generation of CIP initiatives, not only to ensure that CI-based Enterprise Architectures have guidelines and techniques to prevent unwise use of cyber technology for any, and all, control system or incident response applications, but also to provide the focus and incentive for industry and academia to solve those extreme internet, information, and application security issues that are not currently at the top of industry's development agenda.

A TIMELY EXAMPLE

Smart Grid is one example that illustrates many common cyber-physical system risk properties. Smart Grid is an integration of many functional sub-systems, electric systems, cyber systems, control and monitor systems, urban systems, etc., whose purpose is to modernize the entire domain of electric power – from generation to consumption – thereby providing economic and service improvements.

Yet, the improvements facilitated by cyber technology, especially the Internet, create additional vulnerabilities that could be exploited by accident, mischief, Mother Nature, or domestic/international adversaries. Moreover, the assurance of consumer privacy, system-wide stability, and availability and emergency response to regional/national incidents may be compromised in ways that are just beginning to be recognized. Some examples of this predicament include:

- Outsiders and insiders that can exploit vulnerabilities created by the expanded number of component and sub-system interfaces and interactions.
- Hacked information can give thieves opportunities to know when consumers are home, what they are doing; perhaps even interrupting their on-line funds transfer.
- Individual enterprises can be selectively compromised in a myriad of ways, including access to "insider" information.
- Adversaries can interrupt service to communities, national defense interests, commerce, etc.
- Emergency response systems can become as valuable a target as the CI system itself.

Certain system assurance considerations must be folded into a resilient national architecture ahead of system performance features, or risk losing the perpetual leap-frog of putting band-aids on the most recently discovered vulnerabilities. For example, functions with the most severe and irreversible risk consequences may require system architectures that do not employ the Internet as a backbone for inter-connections – particularly certain critical real-time monitor and control processes – until some future date when near-tamperproof sub-systems and components are available. Even a seemingly benign subsystem cannot be secure without fully considering the combinatorial range of other subsystem and intra-system interactions. Therein lays the need for alternate means to accommodate risks that cannot be mitigated with current cyber security technology.

WHAT CAN THE SOCIAL CONTRACT ACCOMPLISH?

The short-term solution is to build new levels of resilience and fault tolerance into the overall national system architecture. The long-term solution is to incubate truly tamper-proof cyber solutions.

How can the Social Contract facilitate national scale resilient architectures?

Until such time as the Internet and alternate system interconnects can be made absolutely secure, their application to combine everything must be limited. Single point failures cannot be inadvertently designed into a national architecture. A truly resilient architecture must isolate detection and warning systems from real-time operational systems, from incident response systems, and so on, to prevent cascading problems from rendering an entire national service unable to defend, operate, or recover. Similarly, better isolation between and among the regional systems would mitigate the cascading effect of local crises into national emergencies. Guidance must be created and adopted to consciously control safe communication among and between such functional and regional subsystems. Everything from application limitations, to interface specifications, to interoperability approaches, to even new public safety spectrum strategies must be considered, simulated, published, and adopted.

These measures must be jointly developed by government and industry, under a program of incentives and regulations that assure adherence.

How can the Social Contract incentivize the development of tamper-proof cyber technology?

The more challenging issue is that extremely secure cyber products are not necessarily the most practical endeavors for industry to pursue. There is ample research that suggests that applications can be made near tamper-proof; networks can have characteristics that provide better detection and near-certain attribution to exploitation attempts, and commercial access control systems can provide classified strength multi-level security protections. However, commercial market dynamics require new products that offer competitive functionality and cost under an ever-decreasing development cycle. Security features are only important to the extent that they meet, or modestly exceed, the competition. R&D programs respond to the price, performance, and time-to-market conditions of the mainstream commercial market. There is the conundrum!

The Social Contract must find innovative ways to provide financial incentives, market protections, and intellectual property rights that "bend the curve" to attract a larger share of American R&D energy to assure the long-term cyber security dominance needed for the nation.

How can the Social Contract gain broad-scale industry and government support?

The Social Contract provides an effective concept to deal with the tension between profit drivers in industry and the needs of people and government. But, as a concept, more is required to implement Social Contract objectives and enjoy Social Contract benefits.

A social contract laboratory environment can be a powerful facilitator by bringing together academic and industrial innovation to meet these cyber security challenges – perhaps even without the administrative, cost and national security protection burdens of "classified"/ mil-spec one-off programs. Together with a prudent program of incentives, a single point of innovation can facilitate solutions beyond those that the market demand would otherwise provide.

The Cyber Security Social Contract Laboratory henceforth referred to as the Social Contract Laboratory (SCL), will encourage and empower industry and government to build a successful relationship through a Social Contract to reduce the impact, and, if possible, to solve cyber security

problems on a broad national scale. As a consequence, not only will technical issues be introduced, but so will many legal and social concerns. In this respect, the services of the SCL will:

- Develop broad acceptance and consensus of the Social Contract approach through confidence in the findings, through methodology, and through the outreach of the SCL and its participants
- Maximize the use of existing technology
- Embrace a sufficiently large problem scope to create useful and safe solutions through one or more well-engineered Social Contracts by empowering, and focusing, the skills and resources of industry and the government
- Discover technology gaps, including gaps in legal and social support
- Evaluate and exercise candidate models of Social Contracts for feasibility, adequacy, and cost effectiveness, especially in terms of time-to-market issues
- Educate and assist industry and government participants to implement, enter into, and perform on a Social Contract basis

The SCL must cover the full lifecycle of Social Contracts regarding cyber security. As such, this laboratory will partner where possible with other organizations and facilities that currently have cyber security-related resources.

The SCL will initially select a “model” critical infrastructure system, for example the Smart Grid, which can be readily and favorably influenced by one or more Social Contracts.

Bibliography

Aerospace Industries Association Annual Conference, *Robert Bigman comments on Cyber Security*, Washington, DC in October 2008

ANSI/Internet Security Alliance, *The Financial Impact of Cyber Risk: 50 Questions every CFO Should Ask*, 2008

Bills, Jeff, *China's Spying Overwhelms U.S. Counterintelligence*, Bloomberg, April 2, 2007

Cross Sector Cyber Security Working Group, *Incentives Subgroup, Incentives Recommendations Report*, September 21, 2009

CyLab, *Governance of Enterprise Security Study*, December 2008

Delloite, *Information Security & Enterprise Risk 2008, Presentation to CYLab Partners Conference*, Carnigie Mellon University, Pittsburg, PA, October 15, 2009

Harris, Shane, "*China's Cyber-Militia*," The National Journal, Saturday, May 31, 2008

Hunt, John, Principle PricewaterhouseCoopers, *Is Cyber Security Improving in the Business World, Why? or Why Not?, presentation on the results of the 2009 Global Information Security Survey*, University of Maryland October 28, 2009

Internet Security Alliance, *The Cyber Security Social Contract: Policy Recommendations for the Obama Administration and the 111th Congress*, December 2008

Nagel, Stewart S., *Handbook of Public Policy Evaluation*, Sage Publications Inc, 2002

National Counterintelligence Executives, *FY07 Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*

Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 2009

PricewaterhouseCooper, The Global State of Information Security, 2008

U.S. Senate, hearing before the Committee on Judiciary, Subcommittee on Terrorism and Homeland Security, *Testimony of Richard Schaffer from NSA*, November 17, 2009

Verizon Business Risk Team, *2008 Data Breach Investigations Report*

White House, *Remarks by President Obama on securing our Nation's Infrastructure*, May 29, 2009

WHAT IS THE INTERNET SECURITY ALLIANCE?

Virtually every corporation has by now integrated the positive aspects of the digital age into their business plan. However, the negative aspects of the informational age including the threats to corporate intellectual property, business operations and overall security have been less appreciated.

The Internet Security Alliance (ISAlliance) is a non-traditional trade association that is designed as a means to understand, integrate and help manage the multi-dimensional and international issues that operating in the Internet age creates.

WHAT DOES THE INTERNET SECURITY ALLIANCE DO?

ISAlliance provides tangible benefits to its membership by creating cutting edge services and applicable across the various industry sectors that use the Internet.

ISAlliance was conceived in conjunction with Carnegie Mellon University to integrate emerging technological issues with the membership's pragmatic business concerns and align public policy to facilitate business growth and resilience.

The ISAlliance provides a broad range of ongoing technological, business and policy services to its membership which can be reviewed at the web site www.isalliance.org

In addition, the ISAlliance Board identifies a select set of priority projects each year for intensive work. In 2008 the ISAlliance has identified the following priority projects:

- The President's National Cyber Initiative (Bush Administration)
- Cyber Policy Development for the Obama Administration and 111th Congress
- Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask
- Developing Automated Security & Assurance for the VoIP Platform
- Securing the Supply Chain in the Age of Globalization
- Applying SAFETY Act incentives to cyber security

Internet Security Alliance
2500 Wilson Boulevard, Suite 245
Arlington, VA 22201

www.isalliance.org

info@isalliance.org

(703) 907-7090