The Internet Security Alliance
answer to the
Department of Commerce Notice of Inquiry: Cybersecurity, Innovation and the Internet Economy

September 20, 2010

Contact: Larry Clinton, President
Phone: 703/907-7090
Email: lclinton@isalliance.org

Executive Summary

Internet Security Alliance comments on the Notice of Inquiry by the US Department of Commerce relative to the economic aspects of cyber security

The Internet Security Alliance (ISA) is a non-profit organization created in 2000 as a collaboration with Carnegie Mellon University. The ISA is a cross-sector organization representing the security interests of major enterprises from the aviation, banking, communications, defense, education, financial services, insurance, manufacturing, security services and technology industries. The ISA's mission is to integrate advanced technology with economics and public policy to create a sustainable system of cyber security.

QUESTION 1 –DEVELOPING A SET OF METRICS ON THE ECONOMICS OF CYBER SECURITY

Research demonstrates that the largest problem with enterprise cyber security is that it is perceived to be too costly. This explains why, despite the vastly increasing attacks on information systems between half and two-thirds of American enterprises are actually reducing their investments in cyber security.

As such the Department's inquiry is extremely timely, however we stress that caution needs to be exercised in developing the needed system of metrics. There already exist ill-defined metrics and general confusion regarding key terms such as security/resilience and "private sector." ISA demonstrates, as does the academic literature that unless a thoughtful conceptual approach—or theory—of cyber security is used to generate the metric model confusion will persist compromising this critical inquiry.

Moreover, we stress that when assessing the issues incumbent in question 1A it is critical to appreciate that government and industry have aligned—but not identical responsibilities. It is the government's job to "provide for the common defense." It is industry's job to maximize shareholder value.

Unless these differing responsibilities are properly appreciated, measuring the "impact" of cyber incidents and the required investments will be compromised. Included in these differences are a number of core economic assumptions which differ significantly between industry and government—and indeed between industry and industry depending not only on the size of the operations but the economic sectors they occupy.

As one of the few organizations which has developed a theoretical structure for enhancing cyber security, and has multiple alliances in the academic, business and government worlds along

with a commitment to enhance overall cyber security on a not-for –profit basis, ISA offers its services to assist the Department of Commerce in this regard.

Question 1C offers an excellent example of the seductiveness of metrics for the sake of metrics as it asks if there are adequate incentives to report breaches. Certainly breaches, at least theoretically can be counted—but the important question is does this information matter? In point of fact there are not adequate incentives to report all breaches, but even if there were it is very doubtful such a "data dump" would enhance overall security.

A more coherent approach to information sharing is providing adequate incentives to provide usable information, which is detailed further in ISA comments.

QUESTION 2 - RAISING AWARENESS

ISA believes that there has been much good work already undertaken to raise awareness regarding cyber security. We believe these efforts may be enhanced by further targeting our efforts, specifically with respect to the business enterprise space.

Although such an effort was urged in the President's Cyber Space Policy Review last year, there has been remarkably little in the way of efforts we have seen in implementing such an approach.

ISA believes that there are three principle issues that need to be addressed in this space. Awareness programs need to be risk management based, enterprise wide, and supported. In our comments, particularly with respect to question 2C ISA provides extensive documentation of the fact that such efforts are not emerging spontaneously, are critically needed and can be highly effective.

Moreover, we identify a detailed and grounded approach to such an effort developed by the ISA in collaboration with the American National Standards Institute (ANSI) and more than a dozen federal agencies.

The program is centered around the fact that in most corporations, although everyone (the HR department, the finance department, the legal department) has data, they generally don't believe it's their responsibility to secure the data. That is up to the, generally underfunded IT department.

The ISA/ANSI program advocates an enterprise wide risk management approach that involves all the relevant players by identifying what cyber security means within their contest and creates corporate mechanisms—generally not in use---to properly analyze, address and financially support required efforts to invest in effective cyber security.

ISA and ANSI are aggressively promoting in numerous ways including the distribution of thousands of free publications and numerous briefings for the corporate community. Should the Department of Commerce wish to join in this private sector effort their support would certainly be welcomed---indeed it may be vital.

In our response to question 2F we present a detailed proposal for the information sharing program alluded to above.

Again, this is a program developed and funded entirely in the private sector and it is being implemented and tested without, to date, any government support---although it would again be welcomed.

The approach, first proposed as part of the development to the Cyber Space Policy Review, and cited within that document, takes a pragmatic and action oriented approach to information sharing as it pertains to the modern day threats of sophisticated attackers using zero-day mechanisms and the APT with clear economic motives.

We find that, while the vast majority of attacks may well be managed by the techniques we identify in our answer to 2C, these determined and sophisticated attackers frankly cannot be stopped from penetrating our systems.

As a result a different strategy needs to be deployed to address these more sophisticated attacks and especially to involve the vast majority of the economy's enterprises who will never be active participants in sophisticate programs like ISA's.

While it may be impossible to defend the infinite Internet perimeter from persistent attackers, once we have them in our systems we have far greater control over them. Moreover we can frustrate the vast majority of these attacks simply not allowing them to escape our networks once they have been compromised---effectively locking the their inside the bank vault. Happily intruders generally need to escape with the stolen data to achieve their ends and they need to register their escape routes in order for them to be part of the global infrastructure. By simply identifying these Command and Control (C-2) web sites and URLs we can develop a system to frustrate even advanced intruders.

In addition, since this information side steps the major reasons entities don't like to share data (no one needs to say they have been breached or give source data) we will increase the incentive for sharing. Finally, by properly placing economic incentives into the model ---based on the model used by the AV industry we can turn this activity into a largely passive one that can readily be embraced even by small companies lacking in the significant IT resources required to participate in current information sharing programs.

QUESTION 4 -7 - WEB SECURITY/AUTHENTICATION/PRODUCT MANAGEMENT/GLOBAL AFFAIRS

ISA provides specific comments on each of these areas, however many of them have intersecting themes that are difficult to summarize given the wording of the questions.

ISA believes that the innovation proposal outlined at the outset of the comments to Question 7 on Research and Development encapsulate many of the more detailed comments in each of the specific questions.

QUESTION 8 INCENTIVES

The ISA does not believe that there are adequate incentives for enterprise cyber security. In fact the economic incentives are generally misaligned from a security perspective.

Perversely, most economic incentives generally, actually favorer the attackers. Cyber attacks are generally easy to launch, inexpensive, can be used to steal immensely valuable data, and the chances of being successfully prosecuted are generally less than 1 in a hundred.

Meanwhile defense is often difficult, expensive (using present models) and return on investment difficult to demonstrate.

ISA has proposed that to remedy this situation a modern "Social Contract" is required built on the principles used to build our infrastructures (telephones and the electric grid) in the last century. In these cases policy makers guaranteed the private investment in these enterprises in return for a broader social good of universal service---we need a similar contract now to assure comprehensive cyber security.

We present a detailed model which articulates how to create a productive industry government partnership with clear roles responsibilities and incentives geared to promoting proven successful cyber security best practices. We highlight how the use of incentives including, but not limited to liability and insurance can be used to create what we seek---a sustainable system of cyber security.

1.) Quantifying the Economic Impact

a) How should a data gathering and analysis system (or systems) be fashioned to facilitate the collection of well-defined, consistent metrics to measure the financial impact of cyber security incidents and investments in cyber security protection?

ANSWER 1A

The importance of this question is underscored by the fact that the research tells us that the single biggest reason corporate information security problematic is the cost of adequate security.[1] The problem is not primarily that we don't know how to secure our networks, it's that we are not investing in doing it.

In their groundbreaking paper "The Economics of Information Security" Anderson and Moore found that "Further externalities can be found when we analyze security investment, as protection often depends on the efforts of many principles. Budgets generally depend on the manner in which individuals' investments translate into outcomes, but the impact of security investment often depends not only on the investor's own decisions but also the decisions of others."[2]

Therefore, to properly develop a system to assess the financial impact of cyber security and the corresponding investments the systems of measurement need to flow from a coherent conceptual approach, or theory, of cyber security, which appreciates the unique characteristics of the subject matter. Metrics in isolation are not sufficient and can be misleading and counterproductive. If metrics alone were the sign of good science, astrology would be the queen of all sciences.

GARBAGE IN GARBAGE OUT—BAD RESEARCH LEADS TO BAD POLICY

There already exists disembodied and simplistic empirical research which if not rigorously examined can lead to misunderstanding and ill-fated public policy.

There needs to be a lot more research before one can quantify exactly what metric are both important and appropriately meaningful for consolidation and comparison on a broad national

[1] McAfee, *In the Crossfire: Critical Infrastructure in the Age of Cyber War*, 2010
[2] R. Anderson and T. Moore, *The Economics of Information Security*. In journal *Science* 314 (2006).

basis. DOC should focus in the near term on promoting examination of those questions through voluntary participation in protected, independent academic studies. There may be lessons learned in some specific work done by the Center for Internet Security (http://cisecurity.org).

For example one recently published, and highly publicized study reported that senior executives currently appreciate an adequate return on investment in cyber security---presumably meaning policy makers have no need to weigh into this area.

One has to look deeply into the fine print of the study to learn that not only is this conclusion based on a remarkably small sample size, but, more damming, a self-selected and biased sample of executives who had recently made substantial investments in cyber security. Executives who had not made such a pro-investment decision were simply eliminated from the research.[3]

The inadequacy of this sort of methodology may explain why the conclusions of this particular study are at dramatic variance from the findings of far larger studies which found that not only don't most executives currently appreciate a business ROI to cyber security investments but, very much to the contrary.

Larger and more rigorous studies demonstrate that notwithstanding the increasing vulnerability and extent of cyber threats, between 50% and 66% of American companies are actually deferring or reducing their investments in cyber security.[4] These latter studies will be treated in more detail in question 3a below.

KEY TERMS NEED TO BE DEFINED

The question specifically calls for the development of a "well-defined" system and thus properly recognizes the importance of properly and clearly specified terms. A key aspect of a technically focused data gathering and analysis system is to ensure a common understanding of terms. A glossary such as NISTIR-7298, Glossary of Key Information Security Terms, should form the common basis for identification of data elements.

In developing the conceptual approach from which the measurement system will evolve there are a number of key terms like "resiliency," "security", "the private sector" and others that need to be carefully modified with appropriate constitutive and operational definitions.

For example, many commentators in the cyber security space have taken to using the terms resiliency and security as though they are synonymous ---they are not.

A resilient system generally is one that can continue to function even under the pressure of attack. However to equate resiliency with security in this context is to assume that the purpose of cyber attacks is always to disable the network.

This is by no means the case. Indeed one of the most serious issues in cyber security is the theft of intellectual property. When this is the goal, be it corporate or government secrets, there is no attempt to disable the network. In fact the continuing functioning of the network/resiliency -

[3] Ponemon Insitute, *U.S. Cost of a Data Breach Study*, 2010
[4] PricewaterhouseCoopers, *Trial by Fire*, 2009. & Center for Strategic & International Studies, *In the Crossfire: Critical Infrastructure in the Age of Cyber War*, 2009.

--continually providing access to proprietary information --may be one of the operating principles of the attack.

In a different context one might consider the cyber security supply chain issues, which are among the most difficult to resolve. Again the notions of resiliency and security are demonstrably misaligned. In the supply chain context a resilient system means that one can continually be supplied (e.g. find parts to build a system or network) from multiple suppliers. However, the more resilient such systems are—i.e. the more different suppliers involved---the less secure the systems become because malicious actors may compromise the supply chain at multiple different locations.

In short, there are many IT supply chains that are extremely resilient, but also extremely insecure. A system of metrics must therefore be very clear about the constructs that are being captured in the metrics; there may be less clarity in this regard with respect to cyber security than is assumed by many policy makers

A similar problem exists with the term “private sector. Put bluntly, there is no unitary “private sector,’ at least not in the same sense as there is a US government. The US government has a single chief executive, unified budget structure and at least theoretically coherent set of goals and objectives.

The private sector conversely is by no means a unity. The private sector is made up of tens of thousands of independent entities with varying and competing goals, structures, cultures and business plans.

Investment decisions, including those for cyber security, are not made by “the private sector” or even an industry sector basis, but rather on the unique needs, goals and budgetary parameters of specific organizations.

Therefore, a set of “well-defined, consistent metrics to measure the financial impact of cyber security incidents and investments in cyber security protection” need to account for this wide variance which goes into the individualized decisions made in assessing the impact of the incidents and investments.

While conceptualizing these metrics on a private sector, or industry sector, basis may be convenient for the unity that is the federal government, such metrics will likely be ill-defined and could be of suspect utility.

WE ARE NOT ALL PLAYING BY THE SAME RULES

In addition to the federal government being a generally unified structure while the private sector is a more diverse one, industry and government also have distinctly different goals and obligations, which, although they may be aligned, are not identical. These differing goals and objectives need to be clearly understood in measuring the impact of cyber events (presumably upon an organization’s goals) and the appropriateness of investment (presumably in pursuit of the organizations goals).

At the most basic level the US Government is constitutionally charged with “providing for the common defense.”

US industry, by contrast is generally, in fact legally, obligated to maximize shareholder value.

While there is certainly an alignment at one level of abstraction between overall national security and shareholder value, it is by no means a one-to-one correspondence and certainly is not understood as such within the Board rooms where the impact of cyber events is measured and the appropriateness of business investment decisions are made.

Indeed it is well known that individual businesses may be willing to tolerate far greater amounts of insecurity than governments may be willing to base on purely economic considerations. For example, various industrial entities tolerate a substantial amount of pilfering rather than upgrading their security if it can be shown the costs of the security upgrades are more expensive than the costs of the security lapses (e.g. retail stores routinely appreciate that a certain amount of their inventory "walks out the back door every month" but finds the investment in security systems to prevent this level of risk to be of greater cost than the cost of enhancing security to prevent it). Governments, dealing with far broader responsibilities may not be nearly as tolerant of risk.

Thus the meaning of, and measuring of, the impact of a cyber incident or the appropriateness of an investment in cyber security could be very different from an industry as opposed to government perspective due to their differing responsibilities with industry far more constrained by issues of cost effectiveness than government.

Moreover, even within the so called private sector it is a mistake to assume that the economic rules affecting cyber security impacts and investment are the same, even among the entities classified as portions of the critical infrastructure. For example, many portions of the critical infrastructures are governed by existing industry government social contracts in which private entities, such as investor owned utilities, make economic decisions with direct influence by government, or quasi government agencies such as public utility commissions. The fundamental economics of these systems is that public policy will guarantee the return on investment to private investors because the enterprises perform a public good that policy makers have determined cannot be provided directly by the government.[5]

In these instances even cyber security investments deemed appropriate for the investor owned utility by its Board of Directors may be deferred or denied for unrelated or political reasons such as a perceived need to restrain consumer prices or simply political pressure to appear to be consumer friendly. Again, regardless of the possible larger picture wisdom of these decisions the fact is that the economics are convoluted and must be clearly understood.

The economics of these portions of the critical infrastructure maybe substantially different from those that govern other aspects of the infrastructure such as the IT or defense sector which do not operate under similar social contracts.

In addition to the greater economic freedom these non-utility sectors enjoy, they also have greater geographic freedom to operate their businesses. Whereas an electric utility or chemical plant may not have the practical ability to move their business to locations, including different countries, which may have better economic environments, the critical manufacturing, IT and even defense industries are not so constrained.

[5] Internet Security Alliance, *The Cyber Security Social Contract: Policy Recommendations for the Obama Administration and the 111th Congress*, December 2008 and *Social Contract 2.0: A 21st Century Program for Effective Cyber Security*, December 2009.

Such movement, made more possible than ever in the new world economy, provides a curb on the power of the US government to demand, such as through regulation, cyber security investment on a sustainable basis or risk losing the jobs and other economic benefits these industries provide domestically. These factors also must be built into a measurement system that purports to analyze cyber incidents and required investment strategies to defend against them.

THERE IS NOT NECESSARILY A DIRECT ALIGNMENT BETWEEN INCIDENTS AND PERCEIVED NEED TO MAKE CYBER SECURITY INVESTMENTS

One of the most common, and simplistic, assumptions made is that if the impact of cyber incidents are sever, than it will naturally follow that adequate investments to stop the attacks. A corollary to this belief is that bad behavior, including inadequate security investments by private corporations will naturally be sanctioned economically and this economic penalty will provide a check on poor cyber security practices.

Such an assumption betrays a misunderstanding of the unique characteristics of cyber security.

To begin with, in the world of cyber security, it is not necessarily the entity that is negligent or culpable that receives the economic penalty for that behavior. Anderson and Moore's review of the literature of information security came to precisely this conclusion noting that "Legal theorists have long known that liability should be assigned to the part that can best manage the risk. Yet everywhere we look we see online risk allocated poorly…people who connect insecure machines to the Internet do not bear the full consequences of their actions …(and) developers are not compensated for costly efforts to strengthen their code"[6]

By illustration consider the case of a poor cyber citizen who does not practice good cyber hygiene. He visits suspect web sites, downloads and opens unfamiliar e-mail and attachments and uses obvious and common passwords which he never alters. Not surprisingly, this person will find their identity stolen.

The thief naturally runs up thousands of dollars in fraudulent charges on our hero's credit cards. Who is responsible for this unfortunate incident and who suffers the economic consequences?

Our sloppy cyber hero will suffer minimal economic damages. The economic damages created by this "bad actor" will in fact be visited upon the bank which holds this individual's credit card which actually bears little or no real culpability for the harms that occur. Moreover, as McCarthy noted in his 2010 study "Retail payment systems exhibit a kind of technical externality. Damage is not contained at one node of the payment network but affects other nodes. Cardholder information might be obtained at one merchant location and used for card fraud at other merchants. In this way, security vulnerabilities in one part of the payment system merchant or processor location potentially affect merchants, cardholders and financial institutions in other parts of the system."[7]

The argument here is not that this sort of consumer protection system is bad or inappropriate. Rather, the argument is that the economic impacts are not correlated with the bad behavior. As

[6] R. Anderson and T. Moore, *The Economics of Information Security*. In journal *Science* 314 (2006).
[7] MacCarthy, Mark, *Information Security Policy in the U.S. Retail Payments Industry*, June 2010

a result a measurement system that seeks to properly gage the impacts of cyber attacks must take into account this counterintuitive reality.

A similar complication occurs when considering corporate security issues associated with the theft of intellectual property. An economic model developed by Kunreuther and Heal notes that security investments can be strategic complements: An individual taking protective measures creates positive externalities for others that in turn may discourage their own investments.[8] Bhum and Katarina termed this the problem of "interdependent risk" in which a firm's IT infrastructure is connected to other entities, so that its efforts may be undermined by failures elsewhere.[9] This correlated risk makes firms under invest in both security technology and cyber insurance, which will be discussed in greater detail in Question 8. Finally Anderson and Moore survey of the literature on information security puts it succinctly "Systems are particularly prone to failure when the person guarding them is not the person who suffers when they fail."[10]

As an example, assume a criminal or rogue state entity may desire to steal intellectual property from a high value target. Accessing the target directly may be difficult because the target organization has made substantial investments to prevent unauthorized traffic from entering its system.

However, since the Internet is characterized by broad interconnectedness the target entity may in fact be connected with other entities which have not made substantial investments. The criminal or rogue entity may attack this weaker element in the system and through that window gain access to the ultimate target.

In this instance, which may describe many attacks in the defense industrial base, the point of the attack and the target of the attack may be entirely different entities. Further, the edge entity that is the point of the attack may not be suffering any economic impact from the attack and thus from this entity's perspective the attack may not be considered a significant incident. Moreover, this entity has little incentive to prevent similar attacks.

On the other hand the ultimate target not only suffers potentially severe impacts notwithstanding its defensive investments---but finds that these investments are in fact being undermined by the entity on the edge which is the point of the attack.

Finally, as suggested above, governments often operate on entirely different economic basis than private entities. Consider the economics of cyber weaponry, for example within the context of compromised supply chains. It's well known that information technology supply chains are usually international in composition and thus highly subject to compromise either via software or hardware compromises.

Attacks on the hardware of military IT supply chains can be especially devastating since once completed the malware may be virtually undetectable until it is activated, which may not come until the weapons system is launched. At that time the malware could be capable of misfiring the weapon system or even having it turn back on the entity that launched it in the first place.

The good news is that this type of hardware based IT supply chain attack is fairly difficult to do and prohibitively expensive in most cases. In fact, most criminal entities would be far more

[8] H. Kunreuther and G. Heal, *Interdependent Security*. In journal of *Risk and Uncertainty* 26, 231 (2003).
[9] A. Arora, R. Krishnan, A. Nandkumar, R. Telang and Y. Yang, *Impact of Vulnerability Disclosure and Patch Availability – An Empirical Analysis*, Third Workshop on the Economics of Information Security (May 2004, Minneapolis, MN)
[10] R. Anderson and T. Moore, *The Economics of Information Security: A Survey and Open Questions*

likely to engage in less expensive, and more resilient, software supply chain attacks to achieve their economic gains.

However, since nation states operate on very different economic assumptions than corporate entities they may be willing to spend exorbitant amounts of money on a single use weapon---as was the case with hundreds of billions of dollars invested for decades to build nuclear weapon arsenals never intended for us. In fact some economist blame this phenomenon as the reason that economists have recently abandoned the study of security. Mastanduno noted that the key reason for the general absence of economic analysis of security issues was that nuclear weapons had basically decoupled national survival from economic power.[11]

Compared to this historic pattern of government investment the sort of investment needed to inserted malware in the hardware of a weapon system supply chain ---that would be uneconomic even form most criminal organizations---becomes economically very reasonable.

Private entities engaged in a risk management approach to managing their own cyber security might find little economic payoff in preventing these hardware supply chain attacks since they are unlikely to affect their own bottom line. Conversely governments may have an extremely high need for vigilance in this area.
In this dramatic instance the government's unique cyber problems are not equally shared by the privet entities that make up the bulk of the supply chain.

As such, analyzing and measuring the impacts of cyber events and the necessary investments to address them is complicated by the differing economics affecting government and industry. Any model developed to measure the effects of events and the required investments to prevent them must affirmatively account for these variables.

b) What would be the appropriate entity to perform collection and analysis of the data?

ANSWER 1B
The one word that would best describe an appropriate entity to perform the collection and analysis of the data would be "multi-dimensional"

As articulated in answer 1A the appropriate entity ought to have a demonstrated appreciation for the unique complexities of the economics of cyber security, as well as an ability to explain them in terms of the data.

The entity ought to either include or have access to the various core perspectives and differing expertise that need to be combined to conduct the required research, development and analysis. These would include academia, the multiple industry sectors which face unique cyber security problems as well as ongoing relationships with many of the government agencies involved in the issue.

The Internet Security Alliance is perhaps uniquely positioned to, with proper financial support to perform the required collection and analysis of data.

ISA was created, and has operated for 10 years, as collaboration between one of the pre-eminent academic institutions in the cyber security field, Carnegie Mellon University, and multiple critical industry segments. Currently the ISA Board consists of not only the Dean of

[11] M. Mastanduno, *Economics and Security in Statecraft and Scholarship*, International Organization, v 52, no 4 (Autumn 1998)

CMU's Computer Science Engineering School but also senior management from the aviation, banking, communications, defense, financial services, insurance, manufacturing, security, and technology enterprises.

Moreover ISA has published both broad based conceptual models for creating a sustainable system of cyber security as well as practical guides for implementing these techniques.[12] Finally ISA has numerous ongoing relationships with aligned organizations that bring their own unique expertise to the ISA programs and projects to enhance worldwide cyber security.

c) Are there adequate incentives for businesses to provide information about security breaches, data security losses, and cyber security investments?

ANSWER 1C

It is not even possible to address the adequacy of incentives for reporting breaches without addressing the underlying premise that providing information on security breaches is even necessary. There can only be two reasons to report breaches. The first is any breach notification law that demands public notification if certain information is exposed. The second is the need for the security community in general to be aware of new or emerging threats.

In the first instance, there is every disincentive for companies to go out of their way to evaluate data losses in a manner that will keep them below the legally-mandated reporting threshold. One can easily see that today. While there are breaches of some sort in every company all too frequently, you seldom see them announced under breach notification laws. The reason is simple. Aside from the legislature's decision that those potentially affected have a right to know, there is no value to the company in reporting. The act of reporting does not trigger any additional assistance they could not otherwise just ask for or contract for without legal or brand risk.

The second instance is more to the point of survey. The unchallenged assumption of reporting breaches to the government (or any other authority) is that the information gleaned will add to the security community's pool of knowledge thus allowing that information to be disseminated for the benefit of all. Unfortunately, the assumption is invalid in several respects.

First of all, the fact that there was a breach is of absolutely no value to the security community at large. The malware characteristics or the attacker's command and control address would be of value if not already known, but both of these pieces of information are independent of whether or not there was a breach. Many sophisticated cyber security organizations routinely obtain new malware or C2 addresses from failed attacks or from open source intelligence. For these organizations, reporting this information to the community does not imply a breach but the community still gets value and is happy to get it. There is no reason for that not to be true for organizations that actually experience a breach. They should be able to contribute to the general body of knowledge without the question of a breach even being raised. Until that happens, there is no upside to reporting what they find.

But let's say everyone did report. Could the government, or anyone else, ever fence off sufficient resources to respond to what would be thousands of reports every day? If every

[12] Internet Security Alliance, *The Cyber Security Social Contract: Policy Recommendations for the Obama Administration and the 111th Congress*, 2008 and *Social Contract 2.0: A 21st Century Program for Effective Cyber Security*, 2009 and *The Financial Management of Cyber Risk, 2010 and The Financial Impact of Cyber Risk: 50 Questions Every CFO Should Ask*, 2008

organization, large and small reported promptly, a significant majority would be duplicative but would still have to be vetted and most would reflect attacks that happened days or weeks ago. It would be much more cost efficient to rely on the elite, sophisticated cyber organizations who are aggregators of their customer's data or who choose to invest in an in-depth cyber analysis capability. This group, if the data could be aggregated, is already positioned to capture a statistically significant sample of attacks and much sooner. The marginal cost of capturing the attacks not seen by this elite far exceeds the value of information they might reveal.

Finally, let's assume for the moment that all organizations that are attacked detect the attacks quickly and report them. Further, let's assume that the government can process all the information and synthesize it into actionable reports. There is still no model today for the information to get out to the vast majority of network owners.

Today's collaboration environment reflects a relatively closed community of elites sharing with elites—and even within the elites there are cliques based on the community of interest, whether that be the Financial ISAC, the DIB, or informal organizations like ShadowServer. The net result is lots of very in-depth, but very narrow, soda straw-size views of the threat. In many cases, the elites try to publish (or sell) the information but the dissemination must almost always be pulled by the recipient who must, in turn, have considerable internal expertise to make use of the information. Such a model will not scale in either the size of the community or the volume of the data. (This is, indeed, the limiting factor for expanding the DIB process beyond the 30 or so elites now involved.) Under this model, the vast majority of network owners in the US will never find the business justification to invest in the people or technology to make use of the work of the elites, yet this same group is most likely to be part of the large botnets from which an Estonia-like denial of service attack would come.

The only threat information dissemination model that works today is the anti-virus model. It works because, for the recipients of the data. it is essentially a passive activity that requires very little internal expertise. The work of the elite anti-virus vendors is disseminated automatically to every customer who implicitly trusts the data without any attempt to validate it or, for that matter, to even understand it.

Until the nation can develop such a passive model for sharing other threat information, any argument that everyone needs to report every victim who falls for a socially engineered e-mail will not be credible. Under that circumstance, there is no positive incentive that exists.

REPORTING CYBER SECURITY INVESTMENTS

Invoking a requirement to report investments will likely not yield useful information for the government. It is almost impossible today to compare apples to apples when evaluating security architectures. There are simply too many options for vendor selection and capability prioritization for any comparison to make sense beyond the general statement that spending more is likely better than spending less. But even that assumption does not hold. Simply fielding a security system—or meeting an industry standard—does not mean that the system is being properly administered or that the results are being acted upon. Thus measuring cyber investment will measure the cost but not the quality of an organization's security posture. The current environment is about COTS and the low cost provider. There is no incentive for the investment [in security]. The government has to be willing to pay more in order to offset the [security] investment.

IMPACT OF INSURANCE

The insurance industry may have a positive role to play here. To the extent that companies must report losses to their insurance carrier who will take into consideration such losses when establishing future premium levels, the existence of a robust insurance industry will provide market place incentives for companies to provide information about security breaches, losses and investments as well as provide incentives to take action to reduce such breaches, losses and investments.

2.) Raising Awareness

There are at least three aspects of cybersecurity awareness that need emphasis. First, the importance of public corporations and other large private and government agencies in including information and data security and privacy risk in enterprise-wide risk management programs that address not only compliance requirements but prioritization based on risk. Large organizations should be encouraged to adopt international standards against which to map their information technology enterprises, and have annual independent assessments conducted to determine how their enterprises stack up against the standards and what needs to be done to make their enterprises more secure.

Second, traditional cyber security awareness training in large organizations needs to be supplemented with spot checks of individual compliance with the security policies of the respective organization, including susceptibility to social engineering attacks. Employees of organizations need to know that systems are in place to test and evaluate compliance with policies and required practices, and regular training (such as common annual updates) need to supplemented with feedback on non-conforming practices and with examples of attempts to subvert the organization's defenses, and lessons learned from other organizations. Awareness efforts that do not have this proactive complement of activities are usually doomed for failure because few will take the awareness lessons seriously if it looks like a check-the-box exercise.

Third, information security personnel need to receive frequent, free, periodic briefings and opportunities to engage in exchange dialogues on real-world exploits security breaches and attempted intrusions so they are up-to-speed in about the evolving nature of cyber threats and attacks. The long term goal should be to require something like continuing education credit requirements.

A specific program Commerce should support that encompasses these core principles and many others is articulated in the answer to question 2e.

a. How effective are existing educational efforts on the need for cyber security?

ANSWER 2A

There are many effective educational efforts currently being promulgated and ISA does not have data to comment on their overall effectiveness.

However, comments from the ISA membership raise at least some questions that may be suitable for analysis.

First, is the awareness programs properly targeted? A great deal of resources are focused on the k-12 group. It bears noting that quite possibly this group of "digital natives" are more aware than the "digital immigrants" who are running the programs.

In addition, secondary, and particularly elementary school teachers---also mostly digital immigrants are already stretched with ever larger class rooms and "No Child Left Behind" requirements. It's worth considering if cyber security ought to be squeezed into curricular that in some cases is not reaching music, PE and in some cases even history and traditional social studies.

In contrast, the immediate problem exists largely in the current workforce, most of who will remain in the workforce for decades.

It is questionable if highly touted initiatives such as k-12 programs and Public Service Announcements (a very TV era method) are a better risk management approach to cyber security than one targeted to the enterprise space---and especially to the senior corporate management space.

This last point will be expanded below.

b. What additional role, if any, should the government play in cyber security education and awareness efforts?

ANSWER 2B

The government is the cornerstone to the activity for propagating cyber security education and awareness. Waiting for the spontaneous growth of a national interest is unpredictable and can possibly lead to ill-formed foundations. Generally speaking, there is a clear expectation of the pubic that the Government will defend the nation against cyber threats, it is appropriate that the government respond to this expectation through leadership of a comprehensive set of initiatives to not mandate private sector actions per se, but rather develop public awareness that leads to attitudes and mindsets that foster effective practices for cyber security. The Government should assist in the development of industry best practices and understand there may be an incremental cost increase as a result of the new [security] practice or process.

So far, with assistance from the Department of Commerce, excellent programs for children and for seniors have been developed and continue to be refined, many of which are addressed in the next question and answer (2C). The same needs to be expanded to cover the remaining age groups as well as private sector organizations and businesses.

The ISA believes that one of the most critical areas of education currently lies in the enterprise arena (also noted in other answers). The current private sector workforce, most of which will remain working for decades to come, is largely uneducated about cyber security. These so-called "digital immigrants." as opposed to today's teenagers and, younger, 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 is 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. The general picture regarding the financial management of cyber risk is not 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."[13]

In subsequent comments, ISA's grounded approach to build an enterprise education program is identified. The Financial Impact of Cyber Risk produced by ISA/ANSI 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." 36 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.

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.

The next step is 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 multidimensional 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 that the Government in partnership with the private sector can launch an initiative to 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.

c. What programs, beyond continuing education for IT professionals, workplace training for users, or curriculum development for K-12 or post-secondary institutions, should be developed?

ANSWER 2C

[13] Carnegie Mellon: CyLab, *Governance of Enterprise Security Study:CyLab 2008 Report*, December 2008

An education program targeted at senior management that demonstrates how to properly analyze cyber risk, and develop an enterprise wide culture of cyber security is needed.

Unfortunately, the sorts of programs identified in question 2c while laudable; suggest excessively narrow view of the cyber security problems we face.

PricewaterhouseCoopers conducts the largest corporate information security survey in the world. Their 2008 study concluded:

> *"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."*[14]

"Cyber Space Policy Review" released by the President in May of 2009 makes this same point.

> *"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. 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."*[15]

Unfortunately, American enterprises are not properly assessing their financial cyber risk and as a result are not making the investment decisions the Cyber Space Policy Review suggests are needed to create and maintain a resilient system of cyber security.

Despite an avalanche of data indicating that cyber vulnerabilities, attacks and loses are mounting at an increasing pace, two recent large scale studies have shown that American companies are actually---and sometimes dramatically-- reducing their investment in cyber security.

PricewaterhouseCoopers 2009 survey reveals that, nearly half (47%) of all the enterprises studied reported that they are actually reducing or deferring their budgets for information security initiatives, even though a majority of respondents acknowledged that these cost reductions would make adequate security more difficult to achieve.[16]

These results are confirmed by a separate large scale study conducted by the Center for Strategic and International Studies released in 2010 which reported that between 2/3 of IT budgets had been reduced often by 15% or more and cuts were even more significant in critical sectors such as Energy, oil and gas where up to 75% reported reductions.

---

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

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

[16] PricewaterhouseCoopers, *Trial by Fire*, 2009.

The CSIS study concluded that "overall cost was the most frequently cited as the biggest obstacle to ensuring security of critical systems followed by lack of awareness." The study also commented "The number one barrier is the security folks haven't been able to communicate the urgency well enough and they haven't been able to persuade the decision makers of the reality of the threat."[17]

The fact is that American businesses are primarily thinking of cyber security as an "IT" problem rather than appreciating it as the enterprise-wide risk management issue that it really is… Moreover there are structural barriers impeding the necessary communication between the IT specialists and the rest of the organization---most notably the senior executives responsible for investment decisions.

Deloitte's 2008 "Enterprise Risk" study concluded that, in 95% of US companies, the CFO is not directly involved in the management of information security risks, and that 75% of US companies do not have a Chief Risk Officer.[18]

The Deloitte study went on to document that 65% of US companies have neither a documented process through which to assess cyber risk, or a person in charge of the assessment process currently in place (which, functionally, translates into having no plan for cyber risk at all).[19]

The Carnegie Mellon University (CMU) CyLab 2010 Governance of Enterprise Security Study concluded: "There is still a gap between IT and enterprise risk management. Survey results confirm that Boards and senior executives are not adequately involved in key areas related to the governance of enterprise security."[20]

The 2008 CMU study also provided alarming details about the state and structure of enterprise risk management of cyber security.[21] The study pointed out that:

- 83% of corporations do not have a cross-organizational privacy/security team.
- Less than half of the respondents (47%) had a formal enterprise risk management plan.
- In the 1/3 of the 47% that did have a risk management plan, IT-related risks were not included in the plan.

The Internet Security Alliance and the American National Standards Institute have developed a model to address this problem. The ISA-ANSI project involved more than 60 private entities and 13 government agencies over a two year period. The results were two publications ("50 Questions Every CFO Should Ask About Cyber Security" and the Financial Management of Cyber Risk").

These publications provide a detailed framework that reviews cyber security on an enterprise wide basis analyzing cyber issues from the unique perspectives of the human resource manager, the operations team, the legal and compliance offices, as well as the risk management and communications operations. The framework provides a

---

[17] Center for Strategic & International Studies, In *the Crossfie: Critical Infrastructure in the Age of Cyber War*, 2009.
[18] Deloitte, *Information Security & Enterprise Risk 2008*, Presentation to CyLab Partners Conference, Carnegie Mellon University, Pittsburg, PA, October 15, 2009.
[19] Deloitte, *Information Security & Enterprise Risk 2008*, Presentation to CyLab Partners Conference, Carnegie Mellon University, Pittsburg, PA, October 15, 2009.
[20] Carnegie Mellon CyLab, *Governance of Enterprise Security Study: CyLab 2010 Report*, June 2010
[21] Carnegie Mellon: CyLab, *Governance of Enterprise Security Study:CyLab 2008 Report*, December 2008

mechanism to better analyze the financial aspect of the issue in a way that can be better understood, managed and invested in by the CFO or other senior executives.

An educational program built on this framework and targeted to senior executives would yield a better understanding of cyber threats and solutions in enterprises. Moreover the "trickle-down" effects on employees throughout the organization, many of whom will take home these lessons to their children could jump start a nationwide enhancement of cyber security.

d. Are existing information sharing mechanisms adequately-resourced but under-utilized?

ANSWER 2D

No. Existing information sharing mechanisms can be and should be improved. The lack of anti-trust exemptions still create a chilling impact on information sharing. In addition, even assuming no anti-trust issue, there is insufficient motivation for the insurance industry to share rate and loss information. Such sharing of information within the insurance industry could provide substantial benefits as it does today arising from such "brick-and-mortar" organizations such as the Insurance Service Organization (ISO) and Underwriter's Laboratory (UL).

e. Does the government adequately assist businesses in the throes or in the aftermath of a cyber incident?

f. Should the government create a cyber security service center to assist the business community in implementing protection measures, sharing information about cyber threats reported by businesses and other sources, and dealing with cyber security incidents that occur?

ANSWER 2F

Yes. In today's cyber security environment there is one inescapable truth. There is no way to prevent a determined intruder from getting into a network so long as one allows e-mail and web surfing –and no business today can survive long 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. It also relies 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.

Moreover, the gaping hole in cyber collaboration (often called information sharing) is that the vast majority of small and medium–sized organizations, both commercial and government, do not participate in these groups or do not have the resources to take advantage of this information when they get it. Unfortunately, for many in critical infrastructure sectors, these small and medium-sized organizations represent a significant portion of our supply chain. We have a vested interest in their success.

Government ought to create a National Cyber Threat Protection Service to implement a disruption strategy more suited to the sorts of attacks most businesses and governments

experience today. This more contemporary model of information sharing will result in a vast increase in the number of enterprises who will receive—and will use---actionable information. It is built on a voluntary process supported by incentives at all levels to make the system function.

The best way to address the new reality of cyber attacks is to recognize that attackers will get into your network and reformulate our defensive actions to detect, disrupt, and deny attacker's command and control (C2) communications back out to the network.

The strategy is an acknowledgement of the fact that there are fewer, and 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 already infiltrated onto our computers. While some of these sites are legitimate sites which have been compromised, the majority are usually new domains registered by attackers solely for the purposes 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 there might be if an employee needs to legitimately go to that site. This strategy can be successful, but it requires a significant investment, unaffordable to most small and medium size entities and many larger ones.

One of the corollaries of recognizing that networks can always be penetrated is a shift in how we measure ourselves. Measuring ourselves against how many intrusions occur becomes a far less interesting. What counts, instead is the intruder's dwell time in our network, or how long an intruder has had access. It's 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.

There are two ways to reduce the dwell time of an intruder. The first is to make a considerable investment in traffic analysis and analytical methods to detect the malicious outbound traffic in a network. Some large organizations have had considerable success in this arena but it has required a large investment that a majority of organizations are not likely to match.

However, the other way to reduce dwell time is a method every organization, large and small, can match--collaboration with other operational entities. If we can take advantage of the good work of other organizations, we are eager to do so. 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, or any number of other forums. But there is no central clearing house for this information or an operationally focused framework for rapid dissemination of this threat information to a broad national audience.

While there is no national-scale framework in place, there is a model that has already proven effective fighting other cyber security problems. The model involves a set of trusted entities developing threat information and reporting voluntarily (with non-attribution) to a central source, which consolidates the information and rapidly disseminates it 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. They simply let the automated processes protect them as a passive service rather than investing in active collaboration—and with much better results.

If this sounds familiar, it's because it is the model used for the highly successful anti-virus and spam filtering industries. We propose that this same model be used to disseminate information on attacker C2 URLs and IP addresses and automatically block outbound traffic to them. If attackers get into your network but cannot get back out the attack is effectively thwarted.

Such a model will have a tremendous impact against botnets and the advanced persistent threat both of whom make heavy use of web-based command and control. While the first wave of their attacks might initially succeed they would be short-lived after the first discovery because of the rapid and automated dissemination of the C2 channels. Subsequent waves would fail completely by virtue of 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 them 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 his cost-benefit calculations. It seems axiomatic that anything that is both simple and inexpensive while forcing this behavior is worth doing on our part.

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 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. Vendors for firewall devices (the term here being used in its most generic sense) 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 traffic analysis. Organizations, be they commercial, private, or governmental, would apply to be certified as Threat Reporters and have their reports of C2 channels 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. Quality would be evaluated by a review of in-house detection and analytical capabilities designed to give *a priori* confidence in their reports' reliability. This would ensure the information the reporters provide is credible and allow for a more rapid automated dissemination process with minimum manual review. Quantity would be measured after certification to ensure the reporter was contributing enough unique threat information to the community to continue to merit the marketing advantage of being a Certified Threat Reporter.

It is important to note that submission of reports by Threat Reporters would not be the same as disclosing breaches required under other laws or agreements. A significant percentage of reports would come from intelligence or 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 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 and 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 their 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 rapidly distributing them to the community of firewall device vendors. By having a central point disseminating the information to all vendors equally we avoid the problem we face with anti-virus today where not all vendors detect all threats. The NCTRC would also de-conflict 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. By this feedback loop a Threat Reporter could be decertified (i.e. no longer have their reports accepted or 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. The question of who operates the clearing house is largely irrelevant so long as everyone in the model trusts them. 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 reporting information to it as industry is. With the large amount of IP threat information the government sees simply because of the size of its network, the absence of threats detected in their 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, reformat it as appropriate for their device, and push it 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, thus giving network owners a wide variety of products from which to select based on their architecture and investment tolerance. The vendors would differentiate themselves from each other not only on price, but also on their speed of updates and value-add services such as the ability of their customers to manually override the lists or their 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 simply do not have the investment dollars to build a detection infrastructure dependent on traffic analysis or the expertise to make use of the various information sharing groups. With this model, though, these businesses could easily, and voluntarily, afford a single device that most already have anyway.

It would, however, now provide an order of magnitude increase in the level of protection by stopping in near-real time many of paths an attacker would use to get back out of the network. For those who had not been compromised yet when updates come out, they 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, it would minimize the length of time when an attacker could access the compromised box and it would identify compromised computers that might otherwise have gone undetected. Best of all, assuming they implicitly trust the system, the organizations employing 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 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 simply monitoring the NCTRC lists. They would be then able to exhibit good internet citizenship by quickly cleaning their systems and working with the NCTRC to be removed from the block list.

A third benefit, although perhaps more appropriate to 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 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 be the basis of a true Common Operational Picture. If every firewall device supporting this model not only blocked the outbound traffic, but also—again, voluntarily—reported back to the Clearing House that there was a blocked C2 attempt 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 report incidents because of the risk of bad publicity, data reported to this COP would not reveal any information beyond the fact that someone on their 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 has been neutralized. But 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 financial community would see the scope of attacks across their community. Or the Department of Defense would see which attacks were unique to them since there might be no detections of specific C2 sites outside of DoD IP space. And all this 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 be certified threat reporters for branding purposes. It shows that they have a robust, capable process and investments to become credible reporters of threat data. There could even be tiered levels for branding purposes based on the volume and accuracy of inputs, i.e. an anti-virus vendor who might report a lot of C2 URLs based on all the malware they get would be Platinum Reporters. A large company with robust internal capabilities might be a Gold level. Managed Security Service providers would be especially eager to participate since the number of C2 channels first reported by them would be a tremendous marketing tool.
2. The Government will greatly benefit by being provided a very large body of C2 URLs and IPs with 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 upfront effort to champion implementation and 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 see 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 IA 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 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 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 have their devices capable of participating in this model. From there it is 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 taken over by an attacker for use as a Command and Control site or 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 as an error or after demonstrating 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 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

This model, if implemented on a national scale, has the potential to be a game changer. For every attack, if a single organization discovered the attack, the entire nation would soon be protected. It 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 later case, someone registering enough domains to operate on the level our attackers operate today would soon gain such a high profile they would be susceptible to other mitigations.

In the end, this 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 proposed in this paper could set a new standard for effective public-private partnership in the Internet Age.

3.) Web Site and Component Security

This area is another that should be informed by the proposed innovation initiative described in general comments above.

a. Should the government alone, the private sector, or the government and private sector collaboratively explore whether third-party verification of Web site and component security is or can prove effective in reducing the proliferation of malware?
b. What would be the implementation challenges in deploying such measures?

4.) Authentication/Identity (ID) Management

Again, the innovation proposal detailed above should include information sharing and collaboration in this subject space. In addition, however, the Department of Commerce should consider an initiative that attempts to address the part of this issue space that is not covered by the National Strategy, namely, the problem of malware on endpoints. The Strategy explicitly does not cover this critically important problem – that malware on endpoints can frequently steal the authentication credentials exchanged to accomplish the authentication. A secure identity management system must address this problem that has manifested itself in innumerable ways, not the least of which is the ACH funds transfer problem that was widely publicized in 2009, that involved malware on computers of financial institution customers that stole the log-in information and was used to steal money from bank accounts. Best practices for secure financial transactions – in fact, any security-significant communication or data exchange – must include the ability to evaluate the other endpoint to see if there is malware and/or to protect the authentication exchange for being compromised.

a. What, if any, federal government support is needed to improve authentication/identity management controls, mechanisms, and supporting infrastructures?

ANSWER 4A

The US government should uniformly implement standards being developed as a result of HSPD-12, including FIPS-201 PIV, PIV-I, as promulgated under NIST and FICAM. All Federal PKIs need to be cross certified with the FBCA. The US government and industry need to reach agreement on standards for both physical and logical Identity Federation, particularly at Level 4 assurance levels, but also at other levels for less critical interaction between citizens and government. Examples include facility access, secure encrypted email and federated portal access. Building upon the government and industry collaboration on PIV-I, future federal government standards should be developed taking commercial interoperability into consideration. A near-term infrastructure improvement would be a secure, centralized PKI directory (LDAP) supporting secure email across Department of Defense and the FBCA (USG & Industry).

b. Do the authentication and/or identity management controls employed by commercial organizations or business sectors, in general, provide adequate assurance?

ANSWER 4B

Basically no. If the current controls were adequate there would not be the significant push for SCRM and CNCI #11. This will of course vary by business sector. Sectors requiring high levels of identity Assurance are likely on par with or even ahead of some Federal entities. Commercial sectors with advanced identity and access management capabilities are aligning their solutions with Federal standards, such as PIV-I.

c. What role should authentication and identity management controls play in a comprehensive set of cyber security measures available to commercial organizations?

ANSWER 4C

Identity assurance and credentialing are fundamental components of a cyber security program. Entities should use OMB 04 04 and NIST 800-63 to formulate an identity assurance framework. Identity is the foundation upon which a defense-in-depth program is built upon.

d. How can the expense associated with improved authentication/identity management controls and mechanisms be justified financially?

ANSWER 4D

OMB 04 04 and NIST 800-63 provide a framework for making the business case. Building safeguards against Level 3 and 4 risks of compromise and loss are a component in justifying the necessary controls and mechanisms. An additional business enabler is Identity Federation, which can provide timely physical and logical access across organizations based upon a high assurance level identity.

e. How can the U.S. Government best support improvement of authentication/identity management controls, mechanisms, and supporting infrastructures?

ANSWER 4E

The USG can establish clear and uniform standards for identity assurance when collaborating with both federal and non-Federal entities. These should be established through consultation with industry experts and set out in a roadmap with achievable milestones for implementation.

Also, in close collaboration with all stakeholders – public and private - implement the recommendations of the President's National Security Telecommunications Advisory Committee.[22]

f. How might government procurement activities best promote development of a market for more effective authentication tools for use by government agencies and commercial entities? Could a private marketplace for "identity brokers" (i.e., organizations that can be trusted to establish identity databases and issue identity credentials adequate for authorizing financial transactions and accessing private sector components of critical infrastructures) fulfill this need effectively?

ANSWER 4F

(See 4 e for the answer to the first question.)There will clearly be a need for trusted third parties to deliver affordable identity management services for entities too small to efficiently provide their own services. Larger entities should have the option of providing their own services which can be certified by federally recognized accrediting entities.

To be effective there must be a behavioral change within the government to accept that with increased SSC requirements an incremental cost increase in the asset is not entirely out of the question. If [the government] wants to promote development and change they must be willing to pay for it. If the procurement practice revolves around lowest cost and not product assurance the market will not respond with higher priced high assurance products.

g. Should the government establish a program to support the development of technical standards, metrology, test beds, and conformance criteria to take into account user concerns such as how to: (1) Improve interoperability; (2) strengthen authentication methods; (3) improve privacy protection through authentication and security protocols; and (4) improve the usability of identity management systems?

ANSWER 4G

Yes, there is a perception that this is happening already today through NIST and FICAM. This question suggests that these efforts are not recognized as applicable to the Federal government as a whole, which would be a concern. This may mean that the NIST/FICAM efforts should be broader or more formalized.

The real issue here is the development of a common supply chain integrity framework. Once there is a framework the given examples will naturally result.

5.) Global Engagement

The problem of global engagement in the cybersecurity space starts with the question that has not been addressed in the U.S. – what are our domestic strategic cyber priorities and how are they affected by or how should they drive what we do internationally? This question needs to be answered in a way that is informed by private sector input.

Accordingly, the key interagency groups that are involved in addressing critical cybersecurity issues need to include ongoing input from private sector representatives, preferably under the CIPAC framework. Those groups are the IPC, chaired by the White House Coordinator (and the subgroups, including the International Subgroup chaired by the State Department), and the

[22] NSTAC Report to the President on Identity Management Strategy, May 2009, http://www.ncs.gov/nstac/reports/2009/NSTAC%20IDTF%20Report.pdf

NCCIC Sub Unified Coordination Group which is tasked under the National Cyber Incident Response System (NCIRP) to provide the Steady State requirements and oversight for the United States' cyber situational awareness/common operating picture and preparedness for a cyber attack. Private sector representation to these groups will provide key input and allow the private sector to have a seat at the table of national cybersecurity preparedness and hopefully will provide visibility to the broader private sector (CI/KR and non CI/KR) of the nation's strategic cyber priority, and related goals, objectives, milestones and metrics.

These activities should inform the work of the International Sub-IPC and collaboration with the nation's closes allies so that together we can prioritize whether and how we drive our national and allied priorities on the international stage.

a. What cyber security-related problems do U.S. businesses experience when attempting to do business in foreign countries?
b. How can the U.S. Government better encourage the use of internationally accepted cyber security standards and practices outside of the United States?
c. Would a set "cyber security principles"' in the area of standards and conformity assessment procedures be useful? If so, what role should the Department of Commerce play in promoting such internationally accepted principles?

6.) Product Assurance

a. Do current U.S. Government product assurance requirements inhibit innovation in or production of security components and/or security-enhanced IT products and systems? If so, what would be the best way to improve the current U.S. product assurance scheme?
b. What, if any, changes need to be made with respect to international product assurance institutions, standards, and processes (e.g., the Common Criteria Recognition Arrangement)?
c. Can useful U.S. Government or international product assurance guidelines be crafted for the current real-world software development environment?
d. What elements would be necessary to develop an effective industry-government dialogue to clarify the product assurance goals and challenges, and identify workable solutions?

Answer to 6D

The inclusion of supply chain security guidelines is critical to overall product assurance. In order to address the issue adequately a framework accounting for the several different stages of development, their technical and legal aspects and the economic interactions must be developed.

The ISA has constructed such a framework for securing the international supply chain for hardware and firmware products and presented it to the Administration as part of the review leading up to the publication of the Cyber space Policy Review which cites the ISA work.[23] This document provides a detailed but concise model answering question 6d.

7.) Research and Development

a. Together with research and development programs at NIST, DOD, and several other agencies, the current unclassified Federal funding in Cyber Security and Information Assurance Research and Development is approximately $350 million per year. How

[23] Internet Security Alliance, *The Cyber Security Social Contract: Policy Recommendations for the Obama Administration and the 111th Congress*, 2008. P.24-27

can the federal government best promote additional commercial and academic research and development in cyber security technology?

We should begin by noting that a critical area for the government to focus on is R&D for innovation.

The broad issue of cyber innovation encompasses more than just the R&D issues raised in this inquiry including authentication/identity management, website/component security, and perhaps even product assurance, however we will address these issues under this more general question.

Innovation and the need and requirements for developing and instituting an approach to promoting innovation, are relevant to each of the major problem areas in cybersecurity, and the development and evolution of information technology, generally. As suggested in the Federal Register notice, promoting innovation is critical to the long-term economic and security posture of the nation. If innovation only encourages R&D and does not facilitate information sharing about exciting new technologies, practices and awareness/training, it will only address part of the long-term challenge.

Given the role of the Commerce department in cyber R&D, and its broader interest in innovation, generally, Commerce should consider developing or at least supporting the development of an information-sharing and collaboration architecture and process to promote cyber innovation in both the CI/KR and non-CIKR areas, and with and across government. There is no system or process in place in the U.S. to facilitate that kind of information sharing across government, much less with the private sector and academia, about cyber security requirements and what technologies contribute most effectively to meeting those (or new) requirements, and where R&D or other development (standards, practices, etc.) is necessary to fill the gaps.

Launching such a capability will help inform government, the private sector, and academia of what the current set of cybersecurity requirements is in particular problem areas (such as identity management, asset discovery, secure web transactions, risk management, vulnerability detection, etc.), whether and to what extent current technologies exist that can meet those requirements (and/or inform the need for additional requirements). This can be a totally voluntary system that can be used by government agencies to inform RFI's and RFP's, and let them know of the existence of cutting-edge technology roadmaps, and inform government R&D.

Part of the problem we face on the innovation front is a failure to recognize that while isolated efforts at innovation are a good thing, we need to make it easier to share information about and leverage the benefits of innovation. In addition to facilitating information sharing about requirements and experience with trying different technologies to address those requirements, it is important to systematize a process that allows and encourages companies – even small and new ones – to provide input on how their technology(ies) can meet the identified requirements. Not just in a Garnter-magic quadrant level of granularity, but with actual specifications on what the respective technology can deliver.

An architecture and process such as envisioned here will actively facilitate and encourage those who buy technologies (or invest in or test technologies) to consider a much wider range of technologies. It will also encourage companies who want to improve their competitiveness to see what the specifications are among their competitors and strive to improve their technologies or develop new ones. Where there are gaps in currently available technologies, the availability

of information through this process can inform R&D spending and it can encourage government and the private sector to partner with one or more smaller companies' whose technologies show real promise to engage in a collaborative technology roadmap.

More specifically, corporate IR&D decisions align to technologies and capabilities expected by the corporation to be needed by the customer. This customer expectation is often gauged by direct interaction with the customer at the agency level. The scope of this interaction can be limited to silo'ed needs and is likely focused on short term needs of the agency without regard to coincidental needs of other agencies. Therefore a consolidated, well known and integrated strategy and roadmap for mission needs and support would enable corporations and sponsors to make better informed decisions on spend corporately and will help to ensure that the overall portfolio of IR&D investments are coordinated and well-aligned to meet research objectives.

i. For IR&Ds that are past the proof of concept stage (higher technology readiness levels or TRLs): One way is to use the United Kingdom engagement model derived from the Technology Strategy Board (TSB). The TSB sponsors programs that provide matching funding to promote the development and commercialization of concepts that have commercial viability. Proposals for this funding must have a business plan and a mechanism for executing that plan. Teams are composed of academic and commercial entities performing cooperative research leading to commercial product development.
ii. For more strategic or lower TRL, budget priorities usually adversely affect long range research so an increase in longer range research that develops industry-academia partnerships would be desirable. These partnerships work together to design and create solutions that provide the next generation of protection while distributing the innovation and the development risk.

The disciplines that require the most research and development resources are in the areas of analytics to provide faster, more robust detective controls. And standards development to facilitate automated control evaluation and management for multi-vendor, dispersed, and diffused applications (e.g. VoIP service).

Finally, the insurance industry potentially has an important role to play here. Providing R&D funds to a to be created insurance information sharing organization similar to ISO (insurance organization services) to fund frequency and severity of losses could prompt more insurers to provide cyber insurance as well as create defacto best practices and agreed upon loss statistics.

b. What particular research and development areas do not receive sufficient attention in the private sector?

ANSWER TO 7B

Advanced Persistent Threat (APT) concerns– With the advancement in level of sophistication of our adversaries' capabilities and techniques, our abilities in prevention, detection and correction have lagged the adversarial growth and sophistication. New techniques in covert channel and data infiltration detection must be developed so that incident response teams can react more quickly on reliably detected events. Further, our ability to reestablish compromised systems as trusted systems on the network at near real time must be developed. The ability to "play through" and continue the mission when under attack will be a critical success factor for many public cloud-based offerings.

Massive Information Management – The development of applications that rely on databases containing petabytes of information is driving the need for improved information management. Issues surrounding data uncertainty, structured queries and protection profiles of large data sets need to be addressed as the complexity and volume of information repositories rapidly grow.

c. What cyber security disciplines most need research and development resources (e.g., performance metrics, availability, status monitoring, usability, and cost effectiveness)?

ANSWER TO 7C

There are several cyber security disciplines/technologies that would benefit from increased funding

i. Systems availability: A means for automated hot recovery preserving availability (no cold restarting).
ii. Configuration management and control: real time configuration assessments (ability to perform scans and vulnerability assessments at line speeds as opposed to off-line speeds.).
iii. Agile defenses that change profile, from an attacker point of view, and provide line speed sensing and queuing (that includes reducing the information density and load), and cyber situational awareness.
iv. Cohesive data protection strategies for data at rest, in motion, and in use. Many suppliers provide solutions today to address encryption of disks and transports but do not have mature solutions for managing the information lifecycle through content discovery, consistent and effective labeling, and then the application of appropriate protection policies based on the resulting content categorization. The inability to protect the actual content at the right levels forces many organizations to protect entire networks, servers, and disks (fixed and portable), which is very inefficient and may create barriers to effective monitoring within their computing environment with such a high percentage of the traffic being encrypted.
v. Cyber Risk Mitigation Metrics– Today's methods and techniques for mitigating risk associated with protection of sensitive data lack clarity as to a risk reduction value for application of a specific countermeasure to a particular designed architecture that may be determined to have a specific weakness. These metrics would be helpful in making business decisions as to which countermeasure should be applied to adequately strengthen data protection. For example, the decision of adding a firewall or improving the strength of authentication to an application housing sensitive intellectual property would be simplified if a risk reduction value could be weighed against the cost to implement either.
vi. Massive Information Management and Data Analytics (described above)
vii. Effective technical supply chain security R&D is also needed.

d. How effective would a federal government-sponsored "grand challenge program" be at drawing attention to and promoting work on specific technical problems?

ANSWER TO 7D

Cyber Challenge programs are extremely important in addressing our most difficult cyber problems but more importantly in developing the human capital of the future required to address cyber security. Programs like CyberPatriot should be recognized and developed more broadly particularly at the high school though college level.

8.) An Incentives Framework for Evolving Cyber-Risk Options and Cyber Security Best Practices

a. Are existing incentives adequate to address the current cyber risk environment?

ANSWER 8A

The short answer to this question is no, there are not currently enough incentives for making the cyber security investments we need.

Although academics working in the field of cyber security have long noted the poor allocation of incentives for adequate cyber security, only recently have large based studies confirmed their initial observations. Anderson and Moore's groundbreaking work "The Economics of Information Security" concludes by noting that: "Many perverse aspects of information security that had long been known to practitioners, but were dismissed as 'bad weather' have turned out to be quite explicable in terms of incentives facing individuals and organization.[24]

The authors follow up work "The Economics of information Security: A Survey and Open Questions notes: "We find incentives becoming as important to dependability as technical design is…Security failure is caused at least as often by bad incentives as by bad design.[25]

The empirical evidence confirming these observations are now overwhelming.

Estimates of the financial business losses from cyber events range from $46 billion[26] to more than $1 trillion in intellectual property theft cited in the President's Cyber Space Policy Review in 2009.[27]

Meanwhile, Symantec, the nation's leading provider of security software, reports that the number of new cyber threats to the Internet jumped nearly 500% between 2006 and 2007, and then more than doubled again between 2007 and 2008. This represents a 1,000 % increase in new threats to corporate Internet users in just 2 years.[28]

On the other hand, two major studies released in this year conducted by PricewaterhouseCoopers[29] and the Center for Strategic International Studies[30] indicate that between half and 2/3 of American companies are deferring or reducing their investment in cyber security despite the fact that attacks vulnerabilities and threats have increased dramatically and are continuing to increase.

Other research is consistent with this finding and suggests about 1/3 of enterprises generally do a very good job adopting effective best practices and have fairly good success combating cyber events.[31]

---

[24] R. Anderson and T. Moore, *The Economics of Information Security*. In journal *Science* 314 (2006).
[25] R. Anderson and T. Moore, *The Economics of Information Security: A Survey and Open Questions*
[26] Congressional Research Service, Report to House Committee on Homeland Security, 2004
[27] Obama Administration, *Cyberspace Policy Review – Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 2009
[28] Presentation to the US Department of Commerce Economic Security Working Group, *Internet Security Threat Report*, January 7, 2010
[29] PricewaterhouseCoopers, *Trial by Fire*, 2009
[30] Center for Strategic & International Studies, In the Crossfire: Critical Infrastructure in the Age of Cyber War, 2009
[31] PricewaterhouseCoopers, *The Global State of Information Security 2006*

While some may choose to bicker about the details of these numbers the overall picture is compelling.

If vulnerabilities, attacks and losses are growing, and investment in cyber security is going down, we have a problem with the incentive structure.

The enormous weight of this evidence belies the simplistic, but often used, analysis that if companies don't invest adequately in cyber security they will simply go out of business. As discussed in some detail in question 1, the "interdependent risk" which categorizes information security issues often means not only that the investment in sound security by some firms is undermined by their connection to less secure systems, but this fact also undermines the basis for adequate cyber security spending in the first place thus creating a vicious circle of misaligned incentives.[32]

These complications and misalignments of cyber security economics are only part of the story. Security can never be absolute. So in analyzing security "adequately" we need to consider the incentives for security in relation to the incentives to overcome security measures on the part of the attackers.

The sad fact is that in the world of cyber security, all the economic incentives favor the attackers.

Cyber attacks are comparatively easy and cheap to launch (one can purchase this facility on the internet for a small amount). The amount of value one can steal, as illustrated in the statistics cited above is enormous and despite law enforcements great efforts chances of being successfully prosecuted are extremely small, with some estimates being less than 1% successful prosecution.

Part of the problem is the seemingly intractable problem of accountability. We don't even know for sure who attacked Google or Estonia, let alone bring them to justice, let alone the thousands of less high profile invasions

So long as the incentives to launch attacks are greater than the incentives to invest in security we will continue to have successful attacks regardless of technological sophistication. As Anderson and Moore observed in the Economics of information Security "As distributed systems are assembled from machines belonging to principles with divergent interests, we find that incentives are becoming as important as technical design in achieving dependability."

This means that any sustainable model of cyber security must be established in a cost effective fashion. Any solution that does not account for cost effectiveness is doomed to fail.

In evaluating the adequacy of incentives it's important to clarify who's who definition of "adequate" are we using.

Again, as the responses to questions 1 illustrate in greater detail, the government may well have a very different definition of adequacy than private entities emanating from the fact that it is the government's legal obligation to "provide for the common defense." As such, governments may have a lower tolerance of risk than private entities who are charged with the obligation to

[32] R. Anderson and T. Moore, *The Economics of Information Security*. In journal *Science* 314 (2006).

maximize shareholder value. Many organizations tolerate substantial security vulnerability, and even losses, because they calculate that the costs of increasing security are not justified.

Further complicating this analysis is the fact that, perhaps to a unique extent, the private sector is now on the front lines of cyber defense. Traditionally government provided for national defense with armed forces. However, cyber attacks, such as those launched against Estonia and Georgia, were visited on private sector entities like banks and utilities.

In the cyber world private sector entities may be inheriting traditional government burdens, such as national defense, which they are not intended, structured or financed to uphold.

Private sector organizations will naturally make investments in security, cyber or otherwise, at a level sufficient to protect their economic self interest. However, as illustrated above, there is no guarantee that the perceived economic payoff for a private organization's security investment will be identical to or sufficient to meet the needs of government entities with very different responsibilities.

In addition, as illustrated above, in answers to question 2, private industry is in the main, not properly analyzing their true financial cyber risk, which also leads to under investment. As proposed above, there are educational steps that ought to be taken to assist in resolving this situation, however until that is accomplished the perceived costs—underestimated as they may be---are what will be used to justify cyber security investment.

As such there may well be a cyber security gap. Should government desire private industry to take on traditional government roles beyond what is justified by their mandate to maximize shareholder value they will need to fill that economic gap.

This is not a completely unusual circumstance. Governments have long paid the private sector to assist in fulfilling traditional government roles in defense through procurement or contractors or privatization.

One of the most enlightened examples of the government creatively using market incentives to fulfill public interest needs occurred at the beginning of the last century when the revolutionary technologies were electricity and telephone service. Originally, these services were provided on a strictly open market basis where only individuals who could be provided this service consistent with the economics of the provider received service.

However policy makers realized that there was public benefit from universal electric and telephone service. Had the government simply mandated that these services be provided investment would have almost certainly dried up and the diffusion of these innovative technologies and their attendant benefits which were largely responsible for the explosion of American wealth and prosperity through the 20th century would never have occurred.

Instead the policy makers of 100 years ago took a more creative path and essentially made a deal—a "social contract" with industry. Government guaranteed the return on private investment in telephone and electricity providers---which then became known as "privately owned public utilities." In return for this substantial market incentive the private utilities then guaranteed the universal provision of telephone and electricity at affordable rates. This is how "rate of return regulation" was born.

The ISA has proposed a similar—not identical—social contract be created in the beginning of the 21st century.

Government needs the private sector to provide enhanced cyber security beyond what is justified by the business needs of most enterprises. Government should deploy arrange of market incentives (though a process described below) sufficient to overcome the cyber security gap which the evidence clearly indicates exists and is rapidly growing.

Perhaps the best news in this regard is that the actual expenditure to fill this gap is not nearly as substantial as one might assume. As will be described in more detail later, several sources and studies have indicated that between 80% and 90% of cyber breaches could be prevented simply by applying existing security practices and technologies. The most recent of these studies was released in August 2010 by the US Secret Service in conjunction with Verizon. That study concluded that 94% of the 900 actual breaches studied could have been prevented by deploying "inexpensive" practices and technologies.[33]

In return for receiving these incentives industry will harden and maintain the nation's cyber security system. This will place the United States in a leadership role in the world wide digital economy akin to that it enjoyed throughout the 20th century. Confidence in digital enterprise carried out here will grow. Investment will flow. Innovation will follow and our citizens will have the confidence in their identities and their government second to nowhere else in the world.

b. Do particular business segments lack sufficient incentives to make cyber security investments?

ANSWER 8B

As we have argued throughout, the definition of "sufficient" is dependent, at least in one sense, on the individual business plan of the enterprise. Some entities may have greater risk tolerance than others and thus less perceived need for cyber security investments. However even in these cases, as also outlined above there is the persistent problem of the "interconnected risk' (see question 1) as well as the problem of an excessively narrow understanding of cyber risk in many enterprises see question 2)

If we are to assume that preventing and mitigating the economic effects of cyber attacks is the determining factor for sufficient cyber investment the Global Information Security Survey conducted by PricewaterhouseCoopers suggests that about 1/3 of the enterprises studied meet that criteria.[34]

By that measure, and not including the interconnected risk and narrow construction problems, 2/3 of businesses lack significant incentives to invest in adequate cyber security.[35]

This finding would be consistent with the other research cited herein documenting that between half and 2/3 of American companies are deferring or reducing their investments in cyber security this year despite the growing awareness of the threat and its effects.

It is also noteworthy that the notion that smaller firms were immune from cyber attacks because attackers would regard them as not worthy enough targets has not been supported by the

[33] Verizon, *2010 Data Breach Investigations Report*
[34] PricewaterhouseCoopers, *Trial by Fire*, 2009.
[35] Center for Strategic & International Studies, *In the Crossfire: Critical Infrastructure in the Age of Cyber War*, 2009.

research. Indeed studies have indicated that smaller and medium sized firms maybe more likely to attack and compromise because they often have not made the cyber investments and thus are easier targets especially for the modernized automated attacks.

Finally, it is worth noting that middle market size companies are especially positioned to lack sufficient incentives as their concerns surround the more immediate issues of paying weekly payroll. Hackers know this well and thus frequently target these companies as a means of attacking larger infrastructure companies whose systems are connected to or dependent upon these smaller and less secure organizations. It is also these smaller organizations that might be most motivated by the requirements of insurance companies.

c. What would be the best way to encourage businesses to make appropriate investments in cyber security?

ANSWER 8C

The short answer is that government needs to develop a system to provide market incentives which will justify the level of cyber security investment government may desire to fulfill its objectives, but that may be beyond the perceived business needs of private enterprises.

While, as we have noted throughout, this answer varies somewhat depending on the specific business entity, in general businesses make investments when the investors, be they private or shareholders, believe that there will be a sufficient economic return on that investment.

Even so called philanthropic or patriotic investments made by business are usually tied to a perception of a longer term, public relations, based economic return on the investment.

As described above, for some enterprises there is a natural congruence between security investments and economic benefits in terms of efficiency etc. In these cases, which the research suggests is about 1/3 of business enterprises studied for example in the PricewaterhouseCoopers information security studies, no additional incentives may be required.

There is a second classification of enterprises which may actually be able to generate an economic return on cyber security investments but, as discussed in question two above, they are not properly appreciating the financial costs of cyber events and thus not making investments that arguably they should. As described in question 2 these organizations may well be reached with an education program targeted to a broader population of senior executives, including CFOs & CEOs instead of just the CISOs and CTOs. A better understanding of the financial impact of cyber risk may well generate additional investment in cyber security.

However, as documented in the answers to question 1, the research shows clearly that in general there are not sufficient economic incentives for the vast majority of enterprises to even maintain their current investments in cyber security notwithstanding the dramatically increasing threat.

There are three main issues that must be addressed in designing a system to create the sufficient incentives for businesses to make cyber security investments not currently justified by their business plans.

1. A mechanism must be developed to determine what sort of behaviors merit incentives
2. Incentives powerful enough to change the behavior of the specific business organizations must be made available to entities who adopt the desired behaviors

3. Mechanisms to assure that incentives are not fraudulently accessed must be developed

The ISA has proposed the model that may be best adapted to this task is the Food and Drug Administration model.

The FDA does not create drugs; it evaluates drugs to measure their efficacy. Moreover, multiple different drugs are routinely deemed acceptable for varying levels of effectiveness, and drugs are often categorized by levels depending on their strength and effectiveness.

For example there are literally dozens of pain medications suitable for over the counter distribution and a higher classification of pain medications are available only with a prescription and still a higher level that are available but only for MD or hospital administration.

A similar situation exists with respect to cyber security. There are multiple sets of standards and best practices designed for similar security purposes. Some of the standards and practices are developed by government entities such as NIST, some by standards setting organizations such as ISO or ANSI and still others set up by smaller and more discrete entities. One reason for the multitude of standards and practices is that there are multiple different systems and configurations of systems and these systems exist for varying purposes operating in various cultures. No one size of standards or practices "fits all."

The key issue for government ought not to be whom or where the standards and practices are developed but, as with the FDA, how well they work.

The "cyber FDA" would be tasked with evaluation standards practices (DHS already has an entity---the SAFETY Act office which evaluates "anti-terror technologies) and determine their level of effectiveness. (A set of already evaluated practices and standards that can be used as an immediate starting point are detailed in answer (f) below).

Private entities would then voluntarily adopt standards, practices, & technologies which have been assessed and graded for their effectiveness.

Private entities can apply for varying levels of incentive based on their use of increasingly higher levels of practices with greater incentives for more stringent processes e.g. a tax credit of 2% for adoption of a class "A" effective set of practices and a 5% credit for a higher graded level etc.

There are already a number of incentives the government uses to promote pro-social action in areas like the environment, agriculture and transportation which can be adapted for use to promote good cyber security behavior. Among these devices are:

- Tax incentives
- Liability benefits
- Insurance
- Government procurement
- SBA loans
- Stimulus grants
- Streamlined regulatory requirements

It is important for government to offer a wide range of incentives as certain categories will be more relevant to discrete organizations. For example, defense contractors or communications

providers may be very interested in procurement advantages while small businesses may be more sensitive to tax credits.

In addition many of these incentive categories can be applied in multiple ways. For example, liability benefits can range from immunity to simply alterations in burden of proof and insurance benefits can range from qualifying for the ability to purchase a policy through applying various discounts to programs for the adoption of carrying levels of security.

The final major aspect is to develop a mechanism to assess compliance with the provisions which merit the market incentives.

For regulated sectors such as chemical, energy utility and telecommunications the existing regulatory structure can be adapted to assess compliance.

The second such mechanism is liability. An entity that applies for an incentive and still has a breach could be found liable for fraud in applying for the incentive.

A broader mechanism to assist with the assessment of compliance with designated effective cyber security behaviors would be a more vibrant cyber insurance industry. As will be discussed in greater detail in the answers to question 7 (j) broader deployment of cyber insurance not only allows a mechanism for promoting good practices, but also provides a private sector funded mechanism for assessing compliance. When insurance companies have their own money on the line they have an enormous economic incentive to assure that the practices they are insuring are in fact being followed which has the concomitant societal advantage of further assuring better cyber security.

d. Are there public policies or private sector initiatives in the United States or other countries that have successfully increased incentives to make such security investments?

e. Are there disincentives that inhibit cyber security investments by firms?

ANSWER 8E

There are several disincentives that inhibit cyber security investment by firms.

First, disincentives to cyber security revolve around an economy of lowest cost where good security engineering often results in a non-competitive product cost. In short there is often an uneconomic trade-off between security and utility and often utility is valued in the marketplace more than security. As a result corporations who must compete in the marketplace to sell their products have a disincentive to add security features which will make their products less attractive to the market.[36]

Second, government exacerbates the problem of lacking security incentives by creating poorly conceived regulatory policy which can be a substantial disincentive to appropriate cyber security investment.

While there are areas of cyber security where regulation can be helpful, such as consumer issues like breach notification and anti-spam requirements, regulation is generally ill suited for the purposes of infrastructure development.

[36] R. Anderson and T. Moore, *The Economics of Information Security*. In journal *Science* 314 (2006).

Ghose and Rajan[37] show how Sarbanes-Oxley, Gramm-Leach-Bliley and HIPPA placed disproportionate burden on small and medium sized businesses. This research also showed that mandatory investment in security compliance creates unintended consequences such as distorting security markets and reducing competition.

Regulation generally retards proactive investment. Policy makers in the early 20th century realized this and thus basically guaranteed the private investment in critical infrastructures to provide telephone and electric service to the nation in return for the social benefit of universal service. We need a similar approach to stimulate the infrastructure investment that will be required to provide universal cyber security.

Regulations, even process regulations, are confined to to looking backward at threats that were prevalent and thus processes that might have ameliorated these common previous threats. Targets responding to contemporary cyber threats need the flexibility to create, and invest in customized strategies to address modern "boutique" attacks.

For example, the M-Trends Report published in April 2010 by Mandiant found that "Classic prevent and detect techniques do not effectively counter the APT (Advanced Persistent Threat). They can easily defeat normal defenses…Panicked reactions tend to cause more harm than good…You need to employ customized response strategies that meet the specific needs of your organization."[38]

Regulatory requirements designed to require compliance with procedures to mitigate once prevalent attacks may be completely ineffective in countering new ones, yet they will still require tremendous investment in terms of scares resources and personnel.

A study by reported by Joshua Corman of 451 Research at the spring 2010 meeting of the Department of Homeland Security's Software Assurance Form and the 2010 Global Security Survey published by PriceWaterhouseCoopers[39] come to the same conclusion namely that a set of redundant audit requirements are displacing the limited corporate cyber security resources thus actually producing counterproductive atmosphere of security.

These reports indicate that as much as 90% of security enterprise spending is being diverted to audit compliance as opposed to actual security concluding "corporations are fearing the auditor, not the attacker" Moreover a study by Risk Management Inc. finds that there is very little coloration between audit compliance and improved security. As result these audit requirements are actually a disincentive to improved security.

Survey respondents to the PWC study also showed they are most concerned about the regulatory environment and the fact that it has become more complex and burdensome. [40] Asked to identify the economic downturn's impact on the security function, CISOs and CIOs identified the same leading impacts as CEOs and CFOs: "a more complex and burdensome regulatory environment."

[37] MacCarthy, Mark, *Information Security Policy in the U.S. Retail Payments Industry*, delivered at Georgetown University Workshop on the Economics of Information Security, June 2010
[38] Mandiant, *M-Trends: The Advanced Persistent Threat*, 2010.
[39] PricewaterhouseCoopers, *Trial by Fire*, 2009.
[40] PricewaterhouseCoopers, *Trial by Fire*, 2009, P.14

Finally, one of the the most critical impediments to the best practice of cyber security is the immense amount of human effort that must be invested each and every day to maintain well-known, effective cyber security controls.

Because humans are involved, mistakes are made and because of the enormity of the task, little effort can be expended to further enhance cyber security posture. Reduction of the human effort to implement, monitor, maintain, and operate best practice cyber security controls is imperative to breaking the industry's current cycle of being "too busy to get better." Reducing this enormous human effort must be achieved through automation and improved tools to better leverage the time, the knowledge and the expertise of the Nation's cyber security professionals to better defend the Nation from cyber attacks. Industry has begun to address some opportunity for automation but, much work still lies ahead.

A solution is not likely to immerge in the market place without government intervention and investment. Solving the problem of effective automation likely requires a combination of tools, techniques and expertise that are disbursed among a large number of private concerns that are not pre-disposed or well-positioned to cooperate. A viable solution will require drawing upon a multitude of academic disciplines and require the infusion of strong subject matter expertise to proceed towards a solution. The right combination of talent is not likely to come together on its own but only through governmental stimulation. Finally, adequate security automation technology simply does not exist today to support an anticipated solution.

A government supported breakthrough in security automation will: 1) enable an immediate increase in the security posture of the Nation; 2) attenuate the severe, unmet demand for additional cyber security professionals; and 3) allow cyber security professionals to invest significant time in forward looking work to further reduce risk and enhance security of the Nation's NIPP sectors. The breakthrough would likely correct a short-term market place inhibitor and allow industry to sustain future innovation on its own.

f. Are there examples of cyber security best practices that have been (or can be) sufficiently tailored to meet the diverse needs of commercial actors outside the critical infrastructure and key resources (CIKR) sectors?

ANSWER 8F

Yes, indeed there is broad consensus that while there are clearly sophisticated attacks such as the APT referenced above, targeting the most critical infrastructures, the vast majority of attacks are not nearly as sophisticated and can be prevented or mitigated through the use of best practices, standards and technologies that have already been identified.

In July 2010 the US Secret Service, in conjunction with Verizon released their Data Breach Report[41] which covered 900 actual security breaches which had compromised over 900 million records.

The Report concluded that 94% of the successful attacks could have been successfully, and comparatively inexpensively, prevented simply by applying previously identified best practices and standards.

These findings are consistent with a range of research from sources including Verizon[42] and PricewaterhouseCoopers[43] as well as testimony from the NSA[44] and CIA ().

[41] Verizon, *2010 Data Breach Investigations Report*

While these findings are impressive it's important not to jump to the conclusion that they provide a silver bullet to the cyber security monster.

As discussed earlier in this question, for these practices to be applied economically they need to be part of a customized system tailored to the unique business plan and posture of the individual organization.

Moreover, while identified best practices may work today, again as discussed elsewhere, so long as the economic incentives for attacking cyber systems remain so strong, attackers will be motivated to continually refine their art.

As a result what policy makers need to create is not a tourniquet to stop the bleeding, but a system of health which can be economically and practically maintained.

g. Should a set, or sets, of best practices be developed to guide commercial organizations' investment decisions? What role, if any, should the U.S. Government play in their development?

ANSWER 8G

As described above, there are already adequate best practices and standards being developed to provide substantial safeguards to information systems. The US government via various entities already play's an active role in their development and should maintain that participation.

However, with possible specialized exceptions for unique systems, the US ought not seek to develop their own standards for use by "American" companies.

In an inherently international economy, a set of "US standards' could create a counterproductive response.

The US government ought to devote their resources to funding the analysis and evaluation of the standards created in the market and the provide incentives for enterprises to implement them as described herein.

h. What are the merits of providing legal safe-harbors to those individuals and commercial entities that meet a specified minimum-security level?

Answer 8H

The federal government can promote cyber-security efforts by creating a Cyber Safety Act that provides safe harbors or other limitations on cyber-security liability, contingent on reasonable efforts to conform to best practices. This would provide a powerful incentive to adopt effective security measures. It would also make the regular security evaluations especially valuable. Precedent for this action may be found in the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, which provides limitations on liability and damages for claims against sellers of anti-terrorism technologies arising out of the use of anti-terrorism technologies, contingent on having liability insurance. The current Safety-Act law while technically applying to cyber-terrorism events is inadequate when applied to cyber-risk for a number of reasons: (1) the

---

[42] Verizon, *2010 Data Breach Investigations Report*.
[43] PricewaterhouseCoopers, *Trial by Fire*, 2009.
[44] U.S. Senate, hearing before the Committee on Judiciary, Subcommittee on Terrorism and Homeland Security, Testimony of Richard Schaffer of NSA, November 17, 2009.

ability to connect a cyber-event with a terrorist group or hostile nation is, as a practical matter, almost impossible absent an admission on the part of the terrorist group, (2) the economic impact of a major cyber event is the same regardless of whether the event is terrorist related, criminally related, a result of negligence on some company's or individual's part, or (most unlikely) of unknown origin.

Nevertheless the Safety Act law and language can be used as a good template for legislation seeking to promote best practices in the area of cyber security by using the very effective "carrot" of limited liability in well outlined and monitored circumstances.

i. Should an entity be required to implement a cyber security plan or meet a set of minimum security standards prior to receiving government financial guarantees or assistance?

j. What role could/should public policy play, if any, in the development of a cyber-risk measurement framework that would be useful in developing insurance products?

ANSWER 8J

Cyber insurance can improve overall cyber security. Cyber insurance increases cyber security by encouraging the adoption of best practices. Insurers will require a level of security as a precondition of coverage, and companies adopting better security practices often receive lower insurance rates. This helps companies to internalize both the benefits of good security and the costs of poor security, which in turn leads to greater investment and improvements in cyber-security.

The security requirements used by cyber insurers are also helpful. With widespread take-up of insurance, these requirements become de facto standards, while still being quick to update as necessary. Since insurers will be required to pay out cyber losses, they have a strong interest in greater security, and their requirements are continually increasing.

As well as directly improving security, cyber-insurance is enormously beneficial in the event of a large-scale security incident. Insurance provides a smooth funding mechanism for recovery from major losses, helping to businesses to return to normal and reducing the need for government assistance.

Finally, insurance allows cyber-security risks to be distributed fairly, with higher premiums for companies whose expected loss from such risks is greater. This avoids potentially dangerous concentration of risk while also preventing free-riding.

PROBLEMS WITH THE MARKET FOR CYBER-INSURANCE

Despite the benefits of cyber-insurance, the market for cyber-insurance is adversely affected by a number of problems.

First and foremost, insurers are afraid of a "cyber-hurricane" – a major disaster resulting in great number of claims. Cyber-hurricanes represent an uncertain risk of very large losses, and as such are very difficult for insurers to plan for. Because computer systems are interdependent and standardized, they tend to be especially vulnerable to correlated losses of this nature. This fear increases insurance premiums, because insurers naturally focus on worst-case estimates of the expected loss from such an event so that they can maintain underwriting profitability. In addition, "cyber-hurricanes" raise a barrier to entry to the insurance market, because an insurer

may be wiped out if a major event occurs before they have built up sufficient cash reserves. Prices for private market reinsurance for cyber-insurers is extremely high as the fear of a "cyber-hurricane" is felt most by the reinsurance community.

Second, although cyber-insurance has been around for more than 10 years, it is still considered a relatively new area and thus insurers are hampered by a lack of actuarial data with which to calculate premiums. In addition to increasing price, a lack of data leads to problems with the risk analysis undertaken by companies when deciding whether insurance against a particular risk is worthwhile. A lack of data also makes cyber-insurance appear less desirable to companies, while simultaneously increasing the price of cyber-insurance. .

PUBLIC POLICY STEPS

Given the public policy benefits that come with widespread adoption of cyber-insurance and the current obstacles to the widespread creation and adoption of cyber-insurance, the federal government should act in order to help counteract the current market failure in the cyber-insurance market. The federal government has a number of measures at its disposal that it may use to improve the market for cyber-insurance, and by doing so help shore up domestic and international cyber-security.

ENCOURAGE INFORMATION-SHARING

The federal government can promote the sharing of cyber-security information by establishing an antitrust exemption to allow insurers to pool data on vulnerabilities and attacks. This would allow insurers and risk managers to create better actuarial models for cyber-risks, reducing insurance premiums and making cyber-insurance more attractive to companies, and therefore increasing the adoption of cyber-insurance. Precedent for this approach may be found in the Year 2000 Information and Readiness Disclosure Act of 1998, which provides a limited exemption from federal antitrust law and the Freedom of Information Act for the sharing of vulnerability information related to the Year 2000 bug. This action would result in the production of a comprehensive and detailed compilation of cyber-security information at no cost to the taxpayer. By reducing the uncertainties currently associated with cyber-risks, it would tend to drive down the supply cost of cyber-security insurance and reinsurance, leading to lower prices and increased coverage rates. Insurance companies are best placed to compile this data, and already require policyholders to report cyber-attacks. This action would help to reduce the current under-reporting problem at no cost.

Further the federal government could encourage and support the creation of an insurance information sharing organization similar to the current ISO (Insurance Service Organization) model or Underwriter’s Laboratory model.

CREATION OF A “CYBER SAFETY ACT” LAW

The federal government can promote the cyber insurance industry as well as cyber-security efforts in general by creating a Cyber Safety Act that would provide, perhaps among other things, that the liability of a certified company for failures of their cyber security (despite the fact that the security has been certified as generally adequate by the relevant authority) is limited to the amount of cyber insurance the company buys. Safeguards would have to put into palace to ensure that companies had to purchase an adequate amount of insurance. Certification would be contingent on reasonable efforts to conform to best practices. This would provide a powerful incentive to adopt effective security measures. It would also make the regular security

evaluations especially valuable.

Precedent for this action may be found in the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, which provides limitations on liability and damages for claims against sellers of anti-terrorism technologies arising out of the use of anti-terrorism technologies, contingent on having liability insurance. The current Safety-Act law while technically applying to cyber-terrorism events is inadequate when applied to cyber-risk for a number of reasons: (1) the ability to connect a cyber-event with a terrorist group or hostile nation is, as a practical matter, almost impossible absent an admission on the part of the terrorist group, (2) the economic impact of a major cyber event is the same regardless of whether the event is terrorist related, criminally related, a result of negligence on some company's or individual's part, or (most unlikely) of unknown origin.

Nevertheless the Safety Act law and language can be used as a good template for legislation seeking to promote best practices in the area of cyber security by using the very effective "carrot" of limited liability in well outlined and monitored circumstances.

RECOMMENDATIONS

1.) Create a Cyber Safety Act that provides safe harbors or other limitations on cyber-security liability, contingent on reasonable efforts to conform to best practices.

2.) Establish an antitrust exemption to promote the sharing of information and data relating to cyber-security. This actuarial data would allow the risks and benefits of a particular cyber-insurance policy to be calculated more accurately, allowing insurers to charge lower premiums and allowing and making cyber-insurance more attractive to risk managers. There would be no associated cost to the taxpayer.

3.) Consider a measure aimed at reducing the fear of a "cyber-hurricane" among insurers. The two best options for doing so are providing incentives for insurers to establish an ISO or UL model organization to share information, and offering a tax deduction encouraging insurers to increase the capital reserves used to pay out cyber-insurance claims.

Appendix A: Complexity

Environment - in a word “complex”.

Consider the environment in which we face the challenge of cyber security. The Internet is what we commonly focus on but the total environment is far more complex than just the Internet and includes

- the collection of networks which openly cooperate in the Internet and the traditional telecommunications networks, which are both huge and international in scope.

But it is even much more than that. It also includes

- the computers, embedded processors and other devices (e.g., SCADA devices) accessible via networks,
- wired, optical and wireless systems,
- huge scale of the legacy installed base,
- complexity in numbers and configurations,
- increasing and often critical interdependencies between cyber and physical,
- increasing numbers and sophistication of applications,
- increasing number and sophistication of attacks and exploits,
- dependence on human beings for systems and enterprise design, installation, operation, maintenance and upgrades,
- dependence on human beings for compliance with policies and procedures in every aspect in which they play a role,
- the terrible compliance and error rates associated with human beings,
- the time phased nature of legacy systems replacement,
- affordability issues,
- international scope of virtually all aspects,
- immature legal frameworks, national and international,
- legislative initiatives that appear out-of-synch with real issues and focused more on an issue-of-the-day reaction,
- government and private sector relationships that are traditionally forced to comply with regulations and rules for either or both an acquisition relationship or a regulatory relationship but do not contemplate or support a partnership of equals,
- corporate general counsels who generally do not understand cyber risk and thus tend to advise against external sharing and collaboration in order to reduce potential liability or other risks they do understand,
- the toughest aspect to define and manage: the culture, which in many respects tends to be highly independent, organizationally protective, individually disdainful and often in denial of either a serious problem or a need for external help,
- and much, much more

The bottom line is it is VERY complex. There are policy, technical, business (or mission) and human factors issues to challenge the best and brightest among us. A near-term, “silver bullet” solution is not even remotely likely. The “solution” will be a constantly evolving and complex mix of policy, technology, training, monitoring, feedback, analysis and adjustment, applied with sound experience and informed judgment in a risk management framework. It will take substantial participation on a continuing basis by a broad spectrum of multidisciplinary professionals in order to have an appropriate impact trend on such a complex environment.

Appendix B: Information Systems Security Board

As stated in the section on awareness above, companies should be encouraged to voluntarily institution information and privacy risk management programs and contract for annual independent assessments of their enterprises.

Toward this end, the government (DOC lead?) should facilitate the formation of something like an entity once recommended by the President's National Security Telecommunications Advisory Committee for a private sector organization then called an Information Systems Security Board. This recommendation is focused on providing an authoritative structure for codifying, evolving and using informed expert judgment to apply the appropriate known standards, practices and other criteria for cybersecurity from among the literally thousands available and emerging. Congress has legislated the responsibility for Federal computer security standards and guidelines to the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). There is no analogous information systems security focal point for the private sector. The need for such an organization was identified by the National Research Council (NRC) as early as 1991. The Information Systems Security Board (ISSB) was a recommendation of the President's National Security Telecommunications Advisory Committee in 1996, aimed at meeting that need. It represented the first major recommendation of the NSTAC which envisioned private sector implementation rather than government implementation. At that time, government saw a need but saw no reason for government to fund it, even with seed money. Unfortunately, it was well before its time and no organization in the private sector took up the challenge to organize the ISSB. Interestingly, major private sector end users who were briefed on the concept at the time supported it whole heartedly.

The ISSB was proposed to perform the following functions for voluntary use in the market place:

- Evaluate and endorse information systems security standards and practices and evaluation/testing criteria developed by the standards community or other recognized bodies, including international bodies.
- Develop or endorse testing criteria.
- Develop and maintain information systems security principles (ISSP).
- Identify areas in which information systems security standards are lacking and new standards need to be developed, working with the standards community to initiate development.
- Develop rating criteria to identify varying levels of security.
- License testing laboratories and auditing organizations to use the ISSB logo and ratings to identify that a product or system meets ISSB endorsed standards, practices and other criteria for the intended type of application or environment. The license would be issued based on application and proof of competence.
- Enhance the understanding of information security issue solutions and promote the use of ISSB endorsed standards and methodologies.
- Issue technical notes to license holders, product developers, and the standards community.
- Establish a process to adjudicate ISSB rules, testing results, and auditing determinations appeals.

The situation has changed radically since 1996. Government has national and international interests to protect and needs voluntary private sector cooperation and collaboration to achieve

them for cybersecurity and homeland security generally. Accordingly, updates to the original recommendation are appropriate in today's environment. For example,

- Government should fund the startup for an updated ISSB
- Government should provide incentives for major "cyberspace" players to support and participate actively in the ISSB.
- A Congressional charter should detail the roles and responsibilities of the ISSB and provide it with authority and accountability. [Note: this is similar, for example, to the Congressional Charter of the American Red Cross for the inherently federal functions which it performs in disaster response activities.]