

Date: April 4, 2008

From: Russell Cameron Thomas, Meritology

To: Commission on Cyber Security for the 44th Presidency, CSIS¹
James Lewis, Senior Fellow and Director
Ashley Rasmussen, Program Coordinator

CC: Rep. James R. Langevin (RI), Chair²
Rep. Michael T. McCaul (TX), Ranking Member²
Douglas Maughn, DHS Directorate for S&T, Cyber Security
Karl Levitt, NSF Directorate for CISE, Cyber Trust

Subject: R&D INITIATIVE FOR INCENTIVE-BASED CYBER TRUST

I am submitting the following analysis and recommendations to the Commission. My goal is to introduce some breakthrough ideas regarding Incentive-based Cyber Trust and a public-private R&D Initiative to make it happen.

I have co-authored a white paper that presents a comprehensive analysis and call to action, with emphasis on a formal research and development initiative:

- 6-page **Executive Summary**
<http://meritology.com/resources/Incentive-based%20Cyber%20Trust%20-%20Summary.pdf>
- 27-page White Paper: **“Incentive-based Cyber Trust – A Call to Action”**³
<http://meritology.com/resources/Incentive-based%20Cyber%20Trust%20Initiative%20v3.5.pdf>
(Includes a detailed discussion of research questions and Initiative design)

Many noted experts have recommended that more R&D is needed for cyber security metrics and incentives. To our knowledge, this “Call to Action” is **the only specific proposal on how such R&D might be organized and accomplished** in partnership between government, industry, and academics, across industry sectors, and even internationally.

Furthermore, our “Call to Action” is unique in defining a unified incentive-based approach that **works across information security, privacy, digital rights, and information protection**. This is essential if we want to recruit the support of all the diverse and sometimes conflicting interest groups: security professionals, lawyers, regulators, privacy advocates, intelligence and homeland security agencies, the computer/internet/communications industry, critical infrastructure sectors such as financial services and energy, and even consumers.

While some elements of Incentive-based Cyber Trust are being developed and commercialized today (e.g. cyber insurance), most critical elements are still unsolved research problems. Even in

¹ http://www.csis.org/index.php?option=com_csis_progj&task=view&id=1101

² House Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology

³ A shorter version of this paper was accepted at a peer-reviewed conference: the International Conference on Information Society (i-Society 2007), hosted by Purdue University Calumet in Hammond, Indiana.

the best case, it might be 3 to 5 years before it becomes a substantial force in the marketplace. **But without a serious R&D Initiative, it might take decades to develop, or might not develop at all.**

While our “Call to Action” does make mention of “Supporting Legal, Regulatory, and Institutional Frameworks” (p. 10), we did not explore the role of the government in depth in the paper. I realize that this is the focus of the Commission. On the following pages, I sketch some ideas on how the US government can jump-start and promote an R&D Initiative:

- 1. Sponsor an invitation-only workshop in Fall 2008 to design and organize an R&D Initiative for Incentive-based Cyber Trust.**
- 2. Allocate funding in FY09 for seed capital for the R&D Initiative, perhaps using earmarks on several agency budgets.**
- 3. Sponsor a test bed for Policy, Regulation, and Incentive Schemes**
- 4. Form a Cyber Risk Information Collection, Pooling, and Disclosure Task Force**

In addition, I strongly recommend that the Commission look at the recent work of the European Network and Information Security Agency (ENISA) and their project on “Analysing Barriers and Incentives for Network and Information Security in the Internal Market for e-Communication”⁴. In particular, I commend for your consideration the fine report by Ross Anderson, Rainer Böhme, Richard Clayton, Tyler Moore: “**Security Economics and the Internal Market**”⁵. Their report does make recommendations for governments and policy makers on many fronts, including some discussion of market mechanisms and research challenges.

I would welcome the opportunity to have in-depth discussions with the Commission on these topics, and also to recruit my colleagues to the cause, as they have much more knowledge and expertise about specific topics.

Thank you for your consideration,



Russell Cameron Thomas
Principal
Meritology (<http://meritology.com>)
Burlingame, CA
Email: russell.thomas@meritology.com

⁴ http://www.enisa.europa.eu/pages/analys_barr_incent_for_nis_20080306.htm

⁵ http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf

Ideas for the US Government’s Role in promoting R&D on Incentive-based Cyber Trust

Background

I am a small business person who has specialized on Incentive-based Cyber Trust over the last few years. I have been collaborating with both industry and academics colleagues through the Securitymetrics.org virtual community and the Workshop on the Economics of Information Security (WEIS).

I learned of your Commission recently when I viewed the House Subcommittee hearing⁶ held on Oct. 31, 2007, titled: “Enhancing and Implementing the Cybersecurity Elements of the Sector Specific Plans”. During the question and answer period for the second panel, both Representatives Langevin and McCaul solicited ideas from the panelists on what Congress and the US Government could do to improve incentives and market mechanisms to improve cyber security, rather than the usual regulatory or penal approach. The panelists offered a few suggestions, but everyone agreed that more input was required.

Overview of Incentive-based Cyber Trust

We define “cyber trust” to include the confluence of information security, privacy, digital rights, and information protection. From the point of view of economics and social behavior, these have become inextricably intertwined.

In essence, the incentive-based approach puts a market price on cyber risk, and also a price on cyber risk information in a way that is roughly analogous to industrial and consumer credit risk rating and pricing. These market prices for risk can then be reflected in various incentive instruments, including cyber insurance or self-insurance, product and service prices, surety bonds, risk pooling contracts, and so on. Once risk is reflected in prices, then stakeholders can make prudent risk management decisions, investments, and tradeoffs.

The incentive-based approach works by sharing the gains (benefits) of cyber trust outcomes in order to align the interests of all stakeholders and mobilize their collective intelligence and creativity. Like other market mechanisms, it should yield solutions that are substantially more efficient and effective than existing approaches – technologies, mandates, penalties, and politics (antitrust) – while also serving as a complement to them⁷.

There are still many fundamental and applied research problems that need to be solved. We need to have good theoretical and operational models of motivation (individuals and institutions), what they value, how they perceive cyber risks and rewards, and how to create incentives to shift those motivations in positive directions. In addition, we need good ways to pool cyber risk

⁶ Joint hearing of the House Subcommittee on Transportation Security and Infrastructure Protection and Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology.

<http://homeland.house.gov/hearings/index.asp?ID=100&subcommittee=12>

⁷ We do *not* propose Incentive-based Cyber Trust as a purely *laissez faire* solution, with no role for regulation, liability laws, disclosure laws, etc. Quite the contrary. The proposal encourages market solutions where the market works best, and makes room for legal and regulatory solutions where they work best.

information for modeling, simulation, and analysis, which is the empirical basis for cyber risk pricing and incentive instruments.

Why an R&D Initiative?

We believe the needed breakthroughs will best be achieved through a formal R&D Initiative. While there are many industrial, non-profit, academic, and government research projects and centers involved in some way, none bring together the required expertise, resources, legitimacy, and long-term commitment necessary. To make this point more tangible, the following inset explores one case of government funded – NSF’s TRUST research center:

NSF’s Team for Research in Ubiquitous Secure Technology (TRUST) is a Science & Technology Research Center that “is focused on the development of cybersecurity science and technology that will radically transform the ability of organizations to design, build, and operate trustworthy information systems for the nation’s critical infrastructure. [...] TRUST is addressing technical, operational, legal, policy, and economic issues affecting security, privacy, and data protection as well as the challenges of developing, deploying, and using trustworthy systems.”⁸

Thus, TRUST *does* have sufficient scope and charter to tackle Incentive-based Cyber Trust. It lists “Economics, Public Policy, and Societal Challenges” as a research challenge category, but this broad scope includes every aspect of economics and policy, not just the incentive-based approach.

In its current form and direction, TRUST is not a “center of gravity” when it comes to research on Incentive-based Cyber Trust⁹. For example, Incentive-based Cyber Trust is not on the list of current research themes¹⁰. The researchers involved are only academic (as far as I can tell), with industry participation limited to sponsorship. There is no major involvement from industrial research organizations in this particular category, no significant involvement from the risk management/modeling/rating communities, and no significant involvement from leading information security consultants or practitioners. There also seems to be little involvement from the Sector Specific Coordinating Councils, who have defined R&D priorities but lack the wherewithal to fund that research or guide it¹¹.

My main point here is that there is no “center of gravity”¹² for research and development for Incentive-based Cyber Trust. Without this “center of gravity”, R&D on Incentive-based Cyber Trust exists only on the margins and in the organization cracks. It’s being done by a few widely distributed individuals with little support from their parent organizations.

To provide this “center of gravity”, we recommend the formation of an R&D Initiative in collaboration with government, industry, and academics. It needs to be radically interdisciplinary, international, multi-institutional, and multi-sector. More specifically, we propose a virtual organization¹³ that leverages existing organizations, centers, and resources, but

⁸ <http://www.truststc.org/>

⁹ This is not a criticism of TRUST. They are fine people doing excellent work. My point is that TRUST is limited in its resources and organization, and is focused in other directions. Furthermore, actual research topics are selected by individual researchers based on their interests and expertise and not by TRUST leadership.

¹⁰ The current TRUST research themes are: Education, Electronic Medical Records, ID Theft & Phishing, Knowledge Transfer, Network Defenses, Policy, Sensor Networks, Trustworthy Systems

¹¹ For example, see the Financial Services Sector Coordinating Council Research Agenda (https://www.fsscc.org/reports/2006/Research_Agenda_Booklet_061108.pdf) and Annual Report (https://www.fsscc.org/reports/2007/annual_report_2007.pdf).

¹² By “center of gravity” I mean institution(s) that provide the resources, legitimacy, and long-term commitment necessary to attract people and organizations to the cause.

¹³ As opposed to a “bricks and mortar” public-private research organization such Semitech.

adds coherence, integration, critical mass, access to resources, and serves as a catalyst for projects and results. It needs to have specific programmatic goals to achieve breakthroughs in incentive-based cyber trust, but without cumbersome bureaucracy and overhead that would inhibit initiative, agility, and fluid collaboration. Some experts have called this form “Open Innovation”¹⁴ and “Creation Nets”¹⁵.

US Government’s Unique Role

The US government can play a unique role in jump-starting and promoting this R&D Initiative. But this will require new thinking, unprecedented collaboration across agencies and innovative funding and contract structures. To promote discussion and to stimulate thinking, I submit the following ideas and recommendations:

1) Jump-start the R&D Initiative

The US Government has already done a good job in defining the need for R&D in cyber risk management and incentive-based approaches. The latest of many examples is the recently updated DHS document: “Coordination of Homeland Security Science & Technology”¹⁶, p. 67-75. What’s missing in all the US Government reports is any leadership or direction regarding *how* to accomplish this R&D and especially how to make it feasible given its public-private, interdisciplinary, international, and multi-sector nature.

Recommendation #1: Sponsor an invitation-only workshop in Fall 2008 focused on designing and organizing an R&D Initiative for Incentive-based Cyber Trust.

The workshop would be focused defining the scope, objectives, structure, funding model, and success metrics for the R&D Initiative. With sufficient pre-workshop preparation and discussions, it might be possible to complete an outline design with a one or two-day workshop.

The US Government would be the key sponsor, perhaps through NSF Cyber Trust, DHS S&T, and/or other agencies. Government sponsored projects and consortia could also serve as sponsors and/or coordinators. Examples include I3P¹⁷ (funded by DHS), TRUST (funded by NSF), AFCYBER, and one or more Sector Coordinating Committees.

One government sponsorship and participation is in place, it should be possible quickly recruit industry co-sponsorship and participation. Special effort should be made to include individuals (entrepreneurs, consultants, lone academics, thought leaders, etc.) who have been working on these issues and ideas for years. Virtual communities such as Securitymetrics.org are a good starting place. Finally, it’s very important to have international participation. There is no reason that a R&D Initiative focused on Incentive-based Cyber Trust should be limited to the US.

It might be tempting to put this workshop in the same “mold” as other workshops on advanced research topics, where academics structure the agenda, make presentations and lead discussions. In this arena, it is just as important to have industry, government policy, and collaboration

¹⁴ <http://www.openinnovation.net/>

¹⁵ <http://www.johnseelybrown.com/creationnets.pdf>

¹⁶ <http://homeland.house.gov/SiteDocuments/20080401143438-63338.pdf>

¹⁷ Institute for Information Infrastructure Protection ([http:// www.thei3p.org](http://www.thei3p.org))

consultants leading, presenting, and contributing. This has been done successfully¹⁸ but requires careful workshop design, participant selection, and facilitation.

2) Earmark seed capital for the Initiative

Money is needed to get this started. Without visible, designated funding from *somewhere*, research efforts will not achieve critical mass. The R&D Initiative will be nothing more than wishful thinking.

Recommendation #2: Allocate funding in FY09 for seed capital for the R&D Initiative, perhaps using earmarks on several agency budgets.

I am specifically talking about *seed capital* whose goal is to fund some of the first steps and (mostly) to attract funding from other sources. It's hard to fit such seed capital into existing funding opportunities. For example, the NSF has annual solicitations for Cyber Trust, including large scale “Centers”. But submissions are limited to academic and non-profit research organizations. Furthermore, the evaluation criteria are based on research outcomes, not seeding a R&D Initiative such as we have described. Another example is HSARPA's recent Broad Agency Announcement (BAA) for Long-term Research in Cyber Security. It has a broad scope and is open to all responsible parties. They also indicate willingness to coordinate with other government agencies who might be sponsors or customers. However, there is no funding in FY08 allocated to this BAA. DHS's FY07 BAA on Cyber Security had only \$3.5 million in first year funding against nine topic areas, of which “cyber security metrics” was one.

In-Q-Tel¹⁹, the new venture arm of the Intelligence community in the US Government, is an interesting and successful alternative funding model. Even though it is non-profit, it operates similar to private venture capital firms. While they focus on entrepreneurial ventures rather than pure or applied research, there might be lessons to learn from their success. Perhaps some “research venture fund” model could be developed and tested for this R&D Initiative.

Since I don't know the first thing about government budgeting and funding, I hesitate to make any specific suggestions. However, it seems appropriate to earmark funds from a wide variety of agencies so the burden doesn't fall too heavily on any one agency. It also encourages cross-agency collaboration from the start. At least that is how it would look to me, an outsider.

A critical success factor is to pick a seed funding model that will attract for-profit research investments from such large private sector players. It's also important to attract non-profit research funding from foundations and even NGOs. This might mean using a matching funds program, or similar. Finally, it would be most desirable to incorporate self-funding and gain-sharing regarding intellectual property created to reward early contributors, entrepreneurs, and for-profit sponsors.

¹⁸ One good example in this domain is the Rueschlikon Conference on Information Policy (2005): “Ensuring (and Insuring?) Critical Information Infrastructure Protection”, www.rueschlikon-conference.org/pressdocs/56_R_05_Report_Online.pdf. It was co-sponsored by Swiss Re and the Harvard University Kennedy School.

¹⁹ <http://www.inqtel.org/>

Once seed capital is in place, members in the R&D Initiative would apply for government research funding through the normal solicitations and channels, including SBIR/STTR for small businesses.

3) Test bed for Policy, Regulation, and Incentive Schemes

Today, nearly all of the cyber trust policy schemes are based on a mandate/compliance/penalty model. FISMA is just one example. There is a very strong temptation to continue to add layer after layer on these mandate/compliance programs, because that is what policy makers and auditors know. This creates organizational and cultural resistance to more radical innovative schemes that have not been tested and validated.

There are a variety of innovative and radical policy/regulation/incentive ideas in circulation, but few if any have been tested. One example is a “cap and trade” scheme similar to pollution emission trading. Before adopting such schemes, stakeholders will want to know, “Does this work? Will it work in crisis situations? When does it break down?” The best way to do this is through a standardized test bed.

DHS has invested in the DETER test bed to accelerate research, testing, and experiments on networked computer security. We need a similar test bed for policies, regulations, and incentives.

Recommendation #3: Sponsor a test bed for Policy, Regulation, and Incentive Schemes.

I suggest starting with a paper-and-pencil methods, group facilitation, and scenario exploration. This has been used successfully for over 50 years in policy evaluation. It was pioneered by RAND and others to help policy makers explore scenarios and alternative futures. It is also widely used in business continuity, disaster recovery, and emergency response communities.

This qualitative manual approach can be augmented selectively with quantitative modeling where it makes sense, especially in stress testing models, etc.

One of the best features of such a test bed is that nearly every type of stakeholder could participate, including members of Congress and their staff²⁰. This ability to “walk a mile in their shoes” can dramatically increase consensus and reduce unproductive conflict in policy debates, and also allow policies to be probed and tested appropriately to minimize the “unknown-unknowns”.

4) Cyber Risk Information Pooling and Disclosure

Nearly all experts agree that some form of mandated disclosure²¹ of cyber events and/or risk will be necessary to support a broad incentive-based approach. By analogy, this is like mandating financial reporting for publicly traded companies, health and safety disclosures for consumer products, and environmental disclosure for organizations that handle hazardous materials.

²⁰ ☺

²¹ This is not the same as vulnerability disclosure, which is a separate issue, and much thornier.

In the risk management world, the most relevant recent example is the Basel II framework for risk management and reporting for large financial services firms. It takes some time to develop such a framework and associated regulations and laws, with special attention on getting the balance right between explicit mandates, supervisory oversight, third-party rating agencies, and private sector prerogative and innovation. Last but hardly least is the need to coordinate across geographic and political jurisdictions.

Recommendation 4 – Form a Cyber Risk Information Collection, Pooling, and Disclosure Task Force

It may take two years to complete, but a Task Force should be able to define a framework for disclosure along with necessary policies, regulations, and laws. It will be necessary to synchronize this framework with existing laws and regulations regarding product liability, shareholder disclosure, information protection, and others. Valuable lessons can be learned from organizations and consultants that have initiated “Social Responsibility” reporting to stakeholders.

It’s also important to incorporate pooling of information about actual incidents, near-misses, and business impact (losses, costs, etc.). It may be that third parties such as rating agencies or insurers become the vehicle for such information pooling, but they will require both regulation and supervisory oversight to assure confidence.

There is already a promising platform in the US Government for cyber risk information collection and pooling called the Security Content Automation Program²² (SCAP). It is a set of standards for collecting and communicating security information. It is currently being defined and deployed across the Federal Government in support of the Federal Desktop Core Configuration (FDCC) initiative. However, it has much wider applicability, both inside and outside the government and it should be promoted as a base-level standard for cyber risk information.

It might be best to start within the financial services industry, since they already have years of experience developing and adopting operational risk measurement and Enterprise Risk Management. (I say this even though the recent crisis in credit markets as exposed significant holes in risk models, especially regarding systemic risk.)

Other candidate industries would be telecommunications, energy, and transportation – all part of the critical infrastructure. The Sector Coordinating Councils would provide useful guidance here, but the best test is to see who steps forward with quality recourses and involvement.

²² <http://nvd.nist.gov/scap.cfm>

Summary

As an addendum to our white paper “Incentive-based Cyber Trust – A Call to Action”, I have provided ideas for how the US government can jump-start and promote an R&D Initiative in this domain.

I have argued that Incentive-based Cyber Trust will not take off anytime soon without a concentrated R&D effort. There is no “center of gravity” in either the public, private, or non-profit sectors. But it needs to be an “open innovation” model rather than a monolithic institution or program.

I have also argued that the US government can play a unique role in giving legitimacy, focus, and seed support for an R&D Initiative that would then attract significant private sector and non-profit sector funding and participation.

Here are my main recommendations for US government action:

1. Sponsor an invitation-only workshop in Fall 2008 to design and organize an R&D Initiative for Incentive-based Cyber Trust.
2. Allocate funding in FY09 for seed capital for the R&D Initiative, perhaps using earmarks on several agency budgets.
3. Sponsor a test bed for Policy, Regulation, and Incentive Schemes
4. Form a Cyber Risk Information Collection, Pooling, and Disclosure Task Force

I look forward to discussing these ideas with the Committee, Congress, or other interested parties.

#