Incentive-based Cyber Trust – A Call to Action

Russell C. Thomas
Meritology
russell.thomas@meritology.com

Patrick D. Amon
Ecole Polytechnique Federale de Lausanne
patrick.amon@epfl.ch

Abstract

Many problems in cyber trust exist at least partially because the people and institutions involved are not properly motivated to solve them. The incentives are often perverse, misaligned, or missing. By improving economic, social, and personal incentives, cyber trust can be significantly improved. The incentive-based approach is based on modern enterprise risk management methods and experiences.

Incentive-based cyber trust includes usability, risk information systems, risk communications, social knowledge, markets, and incentive instruments, along with enabling technology and a supporting legal/ regulatory/institutional framework.

While there is research underway into these problems, it is not happening on sufficient scale, scope, or timeframe necessary to deliver breakthrough commercial solutions soon enough. We propose an initiative to drive breakthroughs for incentive-based cyber trust. An initiative will mobilize more resources (money and people) and create new synergies between existing academic disciplines, institutions, consortia, and interest groups. Most important, it will create a critical mass of the brightest thinkers across the globe, provide platforms for collaboration and innovation, and set bold, motivating goals and targets.

1. INTRODUCTION

The term "cyber trust" means the confluence of information security, privacy, digital rights, and intellectual property (IP) protection in pervasive communications and computing systems. From the socio-economic perspective of risk management, these information risks are interrelated and are becoming more so. A prime example of the cyber trust confluence is the case of Sony BMG Music Entertainment in 2005, who distributed a copy-protection scheme with music CDs that secretly installed a root kit on computers that played the CDs. [1] (A "root kit" can allow someone else to gain and maintain access to your computer system without your knowledge.) This case involved digital rights (ostensibly, Sony's original intent), information security, copyright infringement, and potential privacy violations.

The problem addressed by this paper is that cyber trust is currently deficient largely because of perverse, misaligned, or missing incentives at all levels. Thus, people and institutions involved are not properly motivated to solve cyber trust problems or do what they can to maximize social welfare [2] [3]. The Sony BMG case reveals conflicting incentives for various actors – media companies such as Sony, platform companies such as Microsoft, security companies such as Symantec and McAfee, and consumers [1] [4].

For individual users, security, privacy, and digital rights mechanisms are often hard to use and, therefore, are often not used as intended [5]. Consumers continue to be very worried about privacy violations and identity theft, yet they do not take action to protect their personal information on home computers. [6] [7]

Organization incentives depend on mapping cyber trust to organization performance metrics and decision criteria. A recent survey by the Conference Board [8] found that "most security managers don't know how to map their priorities to business objectives, and most top managers don't understand how security fits into their business objectives." Another factor that makes rational decision-making more difficult is that cyber trust claims made by information and computing technology (ICT) and security vendors are frequently not verifiable or they do not stand up to scrutiny [9]. The result is that the marketplace does not sufficiently reward better security, leading to underinvestment.

Software and media companies struggle to collect license revenue and prevent unauthorized use and piracy [10]. Protecting intellectual property continues to be a high priority in research-driven and publishing industries, yet many organizations suffer loss of confidential information [11].

At a societal level, there are many unresolved cyber trust problems. One example is the debate around the Patriot Act in the US, which shows the tension between national security and law enforcement interests, on the one hand, and individual information security and privacy, on the other hand [12].

The main argument of this paper is that an incentive-based approach to cyber trust will yield solutions that are

substantially more efficient and effective than existing approaches. In essence, the incentive-based approach shares the gains (benefits) of cyber trust outcomes in order to align the interests of all stakeholders and mobilize their collective intelligence and creativity. Our second argument is that the breakthroughs required to achieve incentive-base cyber trust requires a formal Initiative which is interdisciplinary, international, multi-institutional, and multi-sector. We propose a virtual organization that leverages existing organizations and resources, but adds coherence, integration, critical mass, access to resources, and serves as a catalyst for projects and results.

In brief, we believe any comprehensive incentive-based cyber trust system will include the following elements:

- **Usability** – Personal incentives are essentially embedded in the design of cyber trust systems, and especially the usability aspects. These include making it easy and rewarding to do the right things, hard to do the wrong things, and making it clear what the risk consequences are of possible actions. Usability includes technology, people, and processes.
- **Risk information systems –** There is a need for information systems to continuously collect and aggregate operational information related to cyber trust, and then to analyze that data to discover cause-effect relationships between operational metrics and stakeholder value. Models are needed to help stakeholders make forward-looking, value-based decisions based on risk scenarios and trade-offs.
- **Risk communication** – cyber trust and risks should be presented in ways stakeholders can understand and act on, given their perceptions, biases, and level of understanding. This could include anything from simple disclosures to sophistication visualization.
- **Social knowledge –** including reputation systems, peer-to-peer support and sharing, and other products of social networks. It also includes certification and other products of trusted third parties (TTPs).
- **Markets** – mechanisms to draw out information, to discover prices, and to support incentive instruments. Examples that have been suggested include "cap and trade" markets (similar to pollution rights markets), "Zero-day" vulnerability auctions, and prediction markets to draw out the "wisdom of the crowds".
- **Incentive instruments –** including cyber insurance, risk sharing pools, risk-based pricing and other contingent payments, bounties, vulnerability auctions, and rights-based licensing systems.
- **Enabling technology** – cyber trust incentive systems should be widely distributed and embedded in the pervasive computing and communication systems.
- **Supporting legal, regulatory, and institutional framework** – while the incentive-based approach is focused on private market transactions and relationships, there is a need for sufficient legal, regulatory, and institutional support to encourage fairness and systemic trust, and to enforce self-regulation and transparency.

The paper is structured as follows. Section 2 presents background for the incentive-based approach by comparing it to alternative approaches. A vision for the incentive-based approach is presented in Section 3. In Section 4 explores the essential elements in more detail, and their interrelationships. In Section 5, we provide illustrative examples of incentive instruments for various problem situations. Section 6 is a brief sketch of how the Initiative might be designed and managed. Section 7 lists research questions by element. Section 8 discusses start-up issues, especially which industries and sectors might be the best candidates for early adoption and financial support. Section 9 has concluding remarks.

2. BACKGROUND

2.1. Terminology

To clarify the discussion that follows, we offer these definitions of key terms, which may differ from common usage or might be unfamiliar to some readers:

- **"Cyber trust" –** an umbrella term we have borrowed from the NSF[1] to include the confluence of information security, privacy, digital rights, and intellectual property (IP) protection in pervasive communications and computing systems as seen from the perspectives of all key stakeholders – individuals, organizations, technologists, governments, and society. Our discussion of problems and solutions is mostly focused on controlling downside risk, but the incentive-based approach can also incorporate upside benefits, which is important to understand risk taking behavior. In addition, the boundaries of this definition is intentionally fuzzy because the economic and sociological aspects of

[1] The National Science Foundation (NSF) Cyber Trust Program is primarily focused on critical information infrastructure protection [9]. Here we use the term "cyber trust" more broadly to include all computer and communication systems along with any electronic information that is worth protecting.

cyber trust cannot be fully resolved without also considering physical security, digital forensics, business continuity and disaster recovery, regulatory compliance, financial accounting and stakeholder reporting, vendor and contract management, and so on, depending on the context or situation. One of the main advantages of the incentive-based approach is that it offers the potential to draw in all these ancillary functions in a common framework.

- **"Incentive" –** Our definition differs somewhat from the usual economic definition: "In economics, an incentive is any factor (financial or non-financial) that provides a motive for a particular course of action, or counts as a reason for preferring one choice to the alternatives. Since human beings are purposeful creatures, the study of incentive structures is central to the study of all economic activity (both in terms of individual decision-making and in terms of co-operation and competition within a larger institutional structure)." [13] Generally, the incentives we consider are tied to desired outcomes, so that they are a form of gain sharing or shared equity. For purposes of this paper and the proposed Initiative, "incentive" is further qualified to include only positive incentives such as remunerative, moral, and personal incentives. We exclude negative or coercive incentives from this definition because we want to draw on and stimulate "market forces", broadly defined. Market systems normally motivate agents through positive incentives. In contrast, coercive incentives (penalties, etc. for failures to act) are usually administered through non-market processes such as legal, regulatory, or authority institutions. (See Section 2.2.3.)
  Regarding personal incentives, we include them in the definition because they "motivate an individual person through their tastes, desires, sense of duty, pride, personal drives to artistic creation or to achieve remarkable feats, and so on. […] Personal incentives are essential to understanding why a specific person acts the way they do, [...]." [13] Personal incentives for cyber trust can be created and even "traded" through product and service design (usability, features and benefits), social networks, brand affiliation, competitions, recognition and reputation systems, and so on.
- **"Risk management" –** a socio-economic approach to managing uncertain and uncontrollable outcomes, especially when faced with possible events that are hard to estimate and have very bad outcomes [14] [15]. The essence of the risk management approach is to estimate the likelihood and severity of uncertain events and then use these estimates in a rational decision-making framework to guide investments, contingency planning, and other decisions. The general spirit of risk management is to balance the expected value of losses with the costs for mitigating those losses. Risk management does not necessarily imply purely quantitative models or monetary valuations. The sociological aspect of risk management incorporates ideas such as risk tolerance/aversion, bias, risk perception, and motivational dynamics (i.e. how people balance the benefits of risk taking behavior with the potential downside loss) [16]. In this paper and the proposed Initiative, we draw on both the technical and common sense definitions of risk management, as contrasted with other approaches to risk.

2.2. Alternative Approaches

There are a variety of approaches to achieving cyber trust and controlling risk [17] [18], which may be used alone or in combination. We discuss each in turn to set the context for the incentive-based approach.

To be clear, we do *not* argue that the incentive-based approach is the only approach that should be used nor is it always the best approach. It's unlikely that *any* of these approaches will be successful in isolation. However, we do argue that the incentive-based has been under-researched, under-developed and under-utilized compared to the others, and that it should have much higher priority.

2.2.1. Technological approach

This approach basically defines cyber trust as a technical problem and attempts to create various technical solutions. Technology is the prime actor, with human actors either absent, secondary, or serving merely as users of the technology. In the purest form of technology-based approach, there is little or no dependence on organization or social entities other than to permit the technology to be implemented.

In research & development within cyber trust, the field of information security has been dominated by the technological approach. In contrast, R&D for privacy, information rights, and IP protection have been dominated by other approaches (discussed below). However, as computer systems have become more pervasive and integrated, there has been considerable effort to find technology-based solutions to enhance privacy, digital rights, and IP protection.

In essence, the technological approach says, "We can target and subdue the problem with our technology and tools". Its success depends on being able to create and

deploy technology with sufficient power and sophistication to overcome the problem.

2.2.2. Mandates-based approach

This approach basically defines cyber trust as behavior and policy control problem and attempts to create solutions involving explicit mandates emanating from centers of authority. Mandates could take the form of regulations, policies, procedures, rules, laws, codes of conduct, contracts, and the like. Centers of authority could include governments, organizations, leaders (formal or informal), administrators, asset owners, or the legal system. Mandates are mostly enforced through audits or inspections, and may or may not have penalties associated with non-compliance.

The mandates-based approach has historically dominated IP protection, where protection was largely a matter of intra-organization processes and practices. It is also widely used inside organizations to define and implement security and privacy policies. Between firms, mandates are regularly used to achieve cyber trust through such vehicles as Service Level Agreements (SLA) and other contracts. Mandates are often included in purchasing requirements of large institutional buyers. Laws and regulatory agency actions often lead to mandates, directly or indirectly.

In essence, the mandates-based approach says "Do this!", over and over again. One author puts it succinctly: "As nearly any serious security publication will tell you, *security is about control*." [19] The success of this approach depends on being able to define explicit mandates and instructions, and also to audit and enforce compliance in practice.

2.2.3. Penalty-based approach

This approach defines cyber trust as a problem of deviant behavior and lack of will power to resist temptations to cheat or exploit. It attempts to create solutions that involve penalty or liability schemes that cause individuals or institutions pay a heavy price for actionable vulnerabilities or insecure products [20]. Product liability in the US is an example of common use of the penalty-based approach, where civil lawsuits and threat of lawsuits are a prime motivating force to avoid defective products hurting consumers. The penalty-based approach is often used in conjunction with mandates, but not always. Together, they say "Do this or else!". What differentiates the two approaches is that the penalty-based approach emphasizes the negative consequences that will be imposed because of bad outcomes (the "…or else") where the mandate-based approach emphasizes the "Do this…".

In cyber trust, the penalty-based approach has been used for many years in copyright and patent protection and, more recently, in enforcing digital rights to creative works. It is being used more and more by governments to protect consumer privacy. There have been some people who have advocated that product liability law should be applied to information and communications technology (ICT) vendors for information security flaws and vulnerabilities, though nothing has been implemented as yet. [21] [22] [23] [24]

To succeed, the penalty-based approach requires that we be able to clearly recognize and define negative outcomes, define injury magnitude, and assign clear responsibility, and to map cause-effect relationships between responsible parties and the negative outcomes. It also requires a system of meaningful and proportionate penalties, along with adjudication and enforcement mechanisms.

Some people view penalties as "negative incentives", and would advocated including both positive and negative incentives in an incentive-based approach. We disagree for three reasons.

First, negative incentives tend to promote avoidance behaviors, including shirking, blame shifting, and information hiding (both obscuring and misrepresentation), among other things. This is the opposite of what we are trying to encourage.

Second, there is almost no way to craft negative incentives in such a way to ensure or encourage the most desirable outcomes (i.e. optimization). At best, you can hope to avoid the worst categories of outcomes. This is not sufficient for the current cyber trust environment, where we need to encourage innovation and creative adaptation by all stakeholders.

Finally, our incentive-base approach is based on market systems. A major part of the power of market systems is the capability to spawn new and complementary markets that share gains and risks. But market systems almost never "trade" negative incentives. For example, if a bank gets a huge fine for regulatory violation, there is no way for the bank to "share" that penalty with their stakeholders (key employees, partners, vendors, etc.), unless those stakeholders are also penalized by the same regulatory body or court. The same is true for criminal liability or stigma/shame. These adhere to specific individuals who have no way to "share" with the organization they work for. There is no practical way to share negative incentives, especially if you are trying to guide collective behavior toward some global optimum.

The economic impact of potential penalties can be incorporated into the incentive-based approach through the Total Cost of (In)security framework, discussed in Section 5.3, below. However, if incentive instruments need to include non-monetary impacts (e.g. stigma, reputation loss, personal consequences), this would require separate treatment and modeling.

2.2.4. Political approach

This approach defines cyber trust as a problem of power relationships and collective interests. Solutions offered include alliances, coalitions, power-shifting actions (e.g. anti-trust suits), countervailing actions or threats, reciprocal commitments, standardization efforts, and communications to influence public opinion.

While the political approach is rarely used to remedy cyber trust at the level of individual incidents or breaches, it is often recommended for use at a societal level or institutional level to explain or remedy perceived root causes of cyber trust problems. Indeed, many experienced information technology (IT) security professionals and consumer advocates believe that a political approach is *essential* due to entrenched corporate or national interests and actors. Two examples are the Electronic Frontier Foundation (EFF) [25] [26] and recent anti-trust concerns involving Microsoft's new anti-virus software [27].

In essence, the political approach says, "Change the power structure, and good things will follow". Its success depends on knowing what is wrong with the current power structure and defining remedies that will make the environment better and not worse.

2.2.5. Incentive-based approach

This approach defines cyber trust as a problem of motivation and action by individuals and institutions. Motivations shape actions, and are in term shaped by perceptions of alternatives, payoffs, risks, and uncertainties. Solutions offered involve incentives and communication of incentives. Incentives may be tangible or intangible, monetary or non-monetary, fungible or non-tradable. Incentives can be embedded in products and services in the form of ease-of-use or help systems. They can be embedded in social systems in terms of social norms and group membership requirements.

In essence, the incentive-based approach says, "Give key actors a share of the potential gains of cyber trust, and thereby draw on the power of self-interest to drive the right actions." To succeed, the incentive-based approach requires that we have a good understanding of what motivates 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.

To date, the incentive-based approach has only been implemented on a limited basis in security and privacy. Outside of copyright, digital rights, and IP licensing, there has been little success in monetizing the value of cyber trust. Other forms of incentives have been implemented in an ad hoc fashion.

It's very important to note that the incentive-based approach does *not* require the existence of a single global system of incentives or risk measurement. To get started and to develop, there is no pre-requisite for industry-wide, country-wide, or international standards or systems. Even in the case of two parties in a business relationship, there is no need to have a complete or "perfect" measure if their individual or collective cyber risks. All that is needed to get started is for the two parties to have some measure of their *relative* cyber risk across decision alternatives and how *relative* cyber risk is driven by observable metrics. This can form the basis of incentive instruments that are mutually agreeable, fair, reward the right behavior, and aren't easily cheated (For more, see item 1 in Section 5.1).

Therefore, it should be possible to bootstrap incentive-based systems on a small scale and relatively quickly, and then let the creative forces of the market place evolve more sophisticated and interrelated systems.

2.3. Why the incentive-based approach is better

Simply put, the incentive-based approach will be more effective than the alternative approaches in the current fast-changing cyber trust environment. While incentive-based approach is not purely based on market prices and payments, the reason is basically same as the argument in favor of markets over command-and-control in the modern world economy. "In 'The Use of Knowledge in Society' [28], von Hayek argued that the market price mechanism serves to share and synchronize local and personal knowledge, allowing society's members to achieve diverse, complicated ends through a principle of spontaneous self-organization. He coined the term 'catallaxy' to describe a 'self-organizing system of voluntary co-operation'." [29]

If cyber trust involved only interactions between machines, then technical approaches alone might be sufficient. If cyber trust were not so complex, context-dependent, and fast changing, it might be possible to implement command-and-control approaches (mandates, penalties, and/or politics) efficiently and effectively without much concern for incentives. However, this isn't the cyber trust environment we face today.

Consider the fact that it takes months or years to make and implement command-and-control decisions (e.g. policies, procedures, penalties, laws, etc.). The wheels of bureaucracy turn slowly. Unfortunately, the cyber trust environment changes so fast that, by the time those decisions get put into practice, it almost impossible to avoid obsolescence, irrelevance, or unintended consequences. (This phenomena has been called the "Red Queen Effect", after the Red Queen's race in Lewis Carroll's *Through the Looking Glass*, where "It takes all the running you can do, to keep in the same place." [30])

For example, consider the case of RFID-enabled (radio frequency identification) mobile phones with near-field communications (NFC) that are now coming on the market. NFC capability allows these mobile phones to

act as either an RFID device or an RFID terminal under program control. One market force driving adoptions of these phones is to improve customer experience in retail environments, especially for payment and loyalty programs [31]. This opens the possibility for many security and privacy risks [32] [33] [34], especially since consumer awareness of these risks is very low [35].

Now consider all the command-and-control mechanisms (policies, procedures, laws, regulations, and technologies) that have been implemented in the last year or two by institutions and governments regarding mobile phones and other intelligent devices. In every case there will be some definition of "mobile phone" plus assumptions about what they can do and not do. But NFC changes the fundamental nature of mobile phones, effectively giving it the capability to be a credit/debit card *and* potentially like card reader terminal. Phone-to-phone financial transactions can happen without the user actively "picking up the call", so to speak. Did any command-and-control mechanism anticipate NFC phones and the associated risks? If the answer is "no", then either the command-and-control mechanisms will need to change (yet again) or they will face obsolescence, irrelevance, or unintended consequences. At the very least, the introduction of NFC phones will mean that all stakeholders will need to rethink their policies and decisions about mobile phone use [34].

Another problem with command-and-control approaches is unintended consequences, especially in crisis situations.

> "In practice, the technology and procedures that are added to make operations safer and more secure quite often get in the way of getting the work done. Security technology and procedures can introduce so many problems into getting the job done that people learn to circumvent them. Because people are inherently helpful and well motivated to do their work, they develop workarounds to bypass security, not because they are not well trained or motivated, but precisely because they are well trained and motivated. In many cases, they could not accomplish their tasks without violating procedures. This is especially true in crises, where normal routines break down and workarounds are essential. […]
>
> "Sometimes problems occur because the pressures on individuals differ from the stated goals of the organization. When people are asked to follow arduous security requirements while at the same time maintaining efficient and productive work schedules, there can be conflicts." [36]

The examples above demonstrate the limitations of the command-and-control approaches. In contrast, the incentive-based approach is more effective in mobilizing the collective intelligence, collaboration, and creativity of all stakeholders to achieve the best outcomes.

3. VISION

Our starting point for a vision is the NSF Cyber Trust Program vision [37] [38] :

"[…] a society in which networked computer systems are:

- More predictable, more accountable, and less vulnerable to attack and abuse;
- Developed, configured, operated and evaluated by a well-trained and diverse workforce; and
- Used by a public educated in their secure and ethical operation."

This describes the "cyber trust" end result fairly well, though we would change "networked computer systems" to "pervasive computing and communication systems". We also add the following items for the soft side of trust – risk management processes, perceptions, and relationships:

- Managed and used by people who are well informed about information risk and have the ability to manage risk/reward tradeoffs.
- Worthy of public trust, and are the subject of well-founded public perceptions of trust.
- Facilitating trusting and mutually beneficial relationships between people, organizations, and societies.

To complete the vision statement, we all the following items to describe the incentive aspects:

- Easy for people to use and understand, so they are more likely to do the right things rather than the wrong things.
- Provide incentives for individuals and institutions, both positive incentives for good behavior and disincentives for bad behavior.

4. ESSENTIAL ELEMENTS

While the scope of incentive-based cyber trust could be defined many ways, we propose that following elements are necessary to fulfill the vision described above. They all require significant innovation individually, but the big breakthroughs will come when they are integrated both in theory and in practical solutions.

4.1. Usability

Personal incentives are the foundation for any incentive-based approach to cyber trust. In a sense, we can say that personal incentives are embedded in the design of information and communication systems, and

specifically in the usability of their cyber trust features. These include making it easy to do the right things, hard to do the wrong things, and making it clear what the risk consequences are of possible actions. Usability includes technology, people, and processes.

If personal incentives are missing or are in conflict with other incentives, we should expect principal-agent problems (i.e. individuals and organizations may be inclined to bypass or avoid good cyber trust practices, and "principals" incur monitoring and enforcement costs to protect their interests. Efficiency and social welfare both suffer.)

There has been considerable interest and research activity recently regarding usable security and privacy [39] [40]. However, this research is not yet well integrated with other elements of incentive-based cyber trusts. For example, no work has been done to understand how usability affects and is influenced by other incentives. Such a connection is vital since poor usability can undermine all the other incentive systems.

4.2. Risk information systems

It will be necessary to have systems to continuously collect and aggregate operational cyber trust information. Without it, it will be impossible to create efficient and effective incentive systems. There have been many calls for information collection and sharing [41] [42], and various organizations and institutions have been set up for this purpose, including CERT [43], Information Sharing and Access Centers (ISACs) [44] and others [45] [46] [47]. However, these mechanisms almost exclusively focus on operational and technical aspects of cyber trust (vulnerabilities, mitigation, remediation, etc.) and not on the risk management aspects. There is very little empirical data on the social and economic aspects of cyber trust, either for academic researchers or for practitioner in industry or government [48]. The oft-cited CSI-FBI survey [49] has serious methodological short-comings and limitations [148] (i.e. small sample size, not a random sample of the population, no validation that respondents have adequate knowledge to answer the survey questions, etc.), and is therefore not sufficient as a data foundation for incentive-based cyber trust. Only the financial services industry shares information about loss incidents as part of their operational risk management efforts [50], but they typically capture only the largest, most public incidents and this data is usually not granular enough to effectively estimate cyber trust risk.

It will be necessary to analyze that data to discover cause-effect relationships between operational metrics and stakeholder value. Models are needed to help stakeholders make forward-looking, value-based decisions based on risk scenarios and trade-offs. Models will have to cope with many challenging problems of ignorance and uncertainty – an area of active research [51] [52] that has not yet been applied to incentive-based cyber trust.

One example where cyber trust models are needed is in to related cyber trust to corporate spending decisions. Modern corporations make spending and investment decisions within accounting and budget frameworks, which includes categories for current expenses, capital investment, "head count" (a.k.a. employees), ear-marked funds, and fiscal time periods. Furthermore, spending on indirect costs is often determined by ratios to other costs. This budget framework has the effect of dividing cash flows in time and space in a way that works well for most ordinary expenses and investments, but does not fit well the uncertain and contingent world of cyber trust. Therefore, research and development is needed on methods to model the cash flow implications of cyber trust so they map to the accounting and budgeting frameworks. (Cyber trust is not the only aspect of the modern information-driven economy that does not fit into existing the accounting and budgeting frameworks. Other examples include intellectual capital [53], real options [54] and social responsibility [55].)

4.3. Risk communication

Incentives have to be presented to actors in a way that is meaningful and actionable, otherwise they won't work. There is considerable research on the topic of risk perception [16] [56] [57] and risk communication [58], including perceptions, biases, and mental models (i.e. ways of understanding, pragmatics, etc.). Most of this research has been in the context of major health and safety risks. However, very little of this research has influenced mainstream research and development in cyber trust. There has been separate research regarding awareness training and communications, but this has been driven by the institutional training discipline and motivated primarily by the mandates-driven approach. This quote is from a guide for creating security awareness training programs, showing the emphasis on mandates and penalties:

> "An effective IT security awareness and training program explains the *proper rules of behavior* for the use of agency IT systems and information, The program communicates IT security policies and procedures that need to be followed. This must precede and lay the basis for any *sanctions imposed due to non-compliance*." [emphasis added] [59].

Risk communication includes a range of activities from simple disclosures to sophistication visualizations. The major challenges facing risk communication for cyber trust are:

- "Risk" has different meanings at an individual level, organization level, and societal level [18] [60].

- Risks and risk perception are usually very specific to context and systemic performance..
- To influence individual behavior, it's best to give feedback in real-time.
- Risks and risk factors are very interdependent, making the cause-effect relationships very complicated.
- Much of cyber trust knowledge is contingent, tentative, vague, ambiguous, and even contradictory.
- Risk cannot always be measured by a simple numerical scale or value system such as money.
- Prior perceptions and mental models are critical to successful communication and to influence behavior.
- It's hard to avoid diving into technical details that most people find befuddling and taxing.
- There are many social and political obstacles to disclosing information about cyber trust and risks. No business decision-maker wants to look bad or untrustworthy, so there is a natural inclination to avoid disclosing or even learning about breaches of cyber trust.

These challenges make risk communication difficult but not necessarily impossible. In other domains, there has been considerable research and experimentation on innovative ways of communicating complex, context-sensitive, and uncertain information to diverse stakeholders. A few examples include environmental risks and HIV/AIDS [58], effects of fertilizer on waste water treatment [61], and health care reform (SimHealth [62]). These examples point to promising lines of research. In addition, modern computing and graphics technology make it possible to create sophisticated animations, including human emotions [63][64][65] and facial expressions [66], which could be valuable in communicating the affective aspects of cyber trust. (There is even an international standard for facial expression representation: the MPEG-4 standard [67].)

4.4. Social knowledge

Mobilizing social knowledge will be critical to incentive-based cyber trust for two reasons. First, knowledge about cyber trust – vulnerabilities, exposures, incidents, losses, mitigation, cost, and forward-looking estimates and perceptions – are all widely distributed. Cyber trust is very dependent on context. Therefore, only the people in that specific context have the necessary information and perspectives to make proper judgments. Second, cyber trust involves both perceptions and forward-looking estimations of risk and these are social processes. Finally, there may be some elements of incentive-based cyber trust that can only be produced by the "wisdom of the crowds", including valuation of hard-to-estimate risks and best practices.

There has been considerable research on social knowledge systems, and also use in practice, with mixed results. Examples include reputation systems [68], peer-to-peer information sharing [69], pooling expert assessments in the face of uncertainty, bias, and weak signals [70] and other mass collaborations [71]. It also includes certification [72] [73] and other products of trusted third parties (TTPs). However, social knowledge systems have only had a limited effect on improving cyber trust, either because they served a limited community (information sharing) or because the information they produced (certifications) was an erroneous signal for cyber trust [74]. Furthermore, social knowledge systems to date have not been integrated with other incentive-based systems.

4.5. Markets

It has been widely recognized that one of the core economic problems of cyber trust is incomplete markets [2]. Because the economic value of cyber trust is not priced and traded, economic actors can not make rational trade-off decisions, leading to inefficient allocation of resources and less-than-optimal results. (By "markets" we mean trading systems that allow buyers and sellers to exchange goods and/or services, including information.)

Of course, primary markets for cyber trust include the real-world commercial markets where customers pay money to suppliers. However, it's clear that these markets are far from complete or even sufficient. For example, there are markets for information security products and services, but these are rarely "value priced" in the sense that buyers do not know what cyber trust they are getting when they buy each product or service.

But the range of possible markets also includes synthetic and simulated markets that are created specifically to discover prices [75], to draw out the "wisdom of the crowds" (e.g. prediction markets [76]), to rectify "Tragedy of the Commons" problems due to externalities (e.g. "cap and trade" such as pollution rights markets) [77], markets for private information [78] and to draw out information directly related to cyber trust (e.g. "Zero-day" vulnerability auctions [79]). There has been a significant amount of research lately on artificial markets in general, including these examples: artificial trading markets [80], derivative markets for trading macro risks [81] [82], and artificial markets with intelligent agents [83]. Also relevant is the research into pricing non-marketed assets [84] [85] and non-market methods for eliciting value and preferences [86], which bridges the domains of risk information, risk communication, and markets.

Conceivably, it might be possible someday to create be markets for pricing and trading cyber risk itself using

the methods and tools of modern mathematical finance. However, this seems far off in the future since it depends on first achieving the base-level innovations described in this paper.

While many of these proposals and experiments to create more complete markets have been interesting and have broken new ground, they have not achieved practical success or widespread adoption in the cyber trust arena. Furthermore, they are rather fragmented and lack a connection to any overall framework for incentive-based cyber trust. The power of markets is multiplied significantly when they are interconnected in meaningful ways.

4.6. Incentive instruments

We define "incentive instruments" as any social or economic device, mechanism, process, or agreement that explicitly ties payoffs for actors to desirable future states of the world so that those actors are motivated to help bring about those states. A "payoff" could be monetary, near-monetary (e.g. a tradable good or service), or non-monetary-but-valuable (e.g. offer of mutual assistance). The reason incentive instruments are essential is that they put the value proposition of cyber trust front-and-center for each stakeholder. They also open the possibility of side payments, compensation, and other balancing transactions to align the interests of stakeholders.

Examples cyber trust incentive instruments that have been implemented or extensively researched include cyber insurance [87] [88] [89] [90], risk-sharing contracts [91], and "bug bounties" [92] [93]. Since the risks associated with cyber trust are frequently either not insured or are not insurable [94] [95] [96], other risk finance and incentive instruments are worth exploring. Outside of the domain of cyber trust, there has been considerable research on risk sharing pools in developing countries [97] [98] [99], risk-based payments and contracts in supply chain management [100] [101] [102], decision insurance (internal to an organization) [103], and risk sharing in other contexts [104] [105]. Those methods and research results should be applied to cyber trust.

New methods are required for digital rights licensing in an era where it's difficult or impossible to prevent unauthorized copying and distribution [106]. The "Street Performer Protocol" [107] and variants [108] are particularly interesting, since they provide for payment to authors/creators prior to distribution. Other interesting variants include the software completion bond [109] and "Voted Compensation" [110] [111]. With some imagination, these might be applied to cyber trust. For example, the Street Performer Protocol might be applied to the market for vulnerability information, fulfilling some of the same objectives as an auction market without some of the negative aspects.

Rights-based licensing could be also applied to privacy, where each person retains some rights over their personal information. This requires a new legal framework [112] and appropriate rights management collectives [113].

No doubt there are other possible incentive instruments that we have left out. Our main point is that incentive instruments are possible and they offer attractive properties to improve cyber trust in the pervasive computing/communications environment. We believe that the space of possibilities has hardly been explored and many innovation opportunities await discovery and evaluation.

4.7. Enabling technology

It's obvious that any incentive-based cyber trust scheme would need support from technology. The design of enabling technology is a serious engineering task that is beyond the scope of this paper. However, we want to make some comments about its characteristics and feasibility.

First, the incentive systems should be widely distributed and embedded in the pervasive computing and communication systems. They should not be a "bolt-on" and completely external to the computing and communications systems they apply to. The logic behind this requirement comes from the context-dependence of cyber trust and the need for significant amounts of real-time information (see Section 4.2). Enabling technology for cyber trust is already becoming pervasive in several domains, including software updates [114] [115] and digital rights management [116] [117], but it is subject of much controversy since it appears that this enabling technology enforces rights of some actors at the expense of others [118]. Indeed, the pervasive and somewhat hidden character of Windows Vista DRM has caused uproar recently [119] because of its alleged impact on PC total cost of ownership and consumer value, even for non-Windows PCs.

These examples show that it is certainly possible to embed enabling technology for cyber trust. What is blatantly missing to date is any meaningful or compelling support for incentive-based cyber trust in the latest versions of enabling technology. This development and commercialization trend will certainly continue unless there is a compelling alternative.

Second, the enabling technology needs to present incentive signals to actors at the right times, i.e. when it will have the most effect on behavior and performance. For individual users, this will often mean giving feedback in real-time as they use their systems and devices so they can make informed decisions about risky behavior and to shape their trust expectations [122]. For buyers and other decision-makers, this means presenting cyber trust signals

in ways that fit the purchase, investment, and implementation decision-making process [8] [120] [121].

Finally, significant innovation is needed regarding how cyber trust information is communicated to avoid the problems such as user confusion [122] or threat level codes [123], to give just two examples. This might draw on technologies for animation, among others. (See Section 4.3 for more on the need to communication in ways that actors are able to act on.)

4.8. Supporting legal, regulatory, and institutional framework

In addition to enabling technology, it's necessary to have a supporting framework of laws, regulations, and institutions. Designing and implementing such a supporting framework is a huge task, requiring significant powers of influence and persuasion, among others. We have already mentioned some of these requirements, above, and we will only provide a brief discussion to suggest the sort of framework that is required.

The best analogy to draw on is the existing framework for modern financial markets (the "free market framework"). The laws, regulations, and supporting institutions are set up to facilitate fairness and trust primarily through self-regulation and transparency. Oversight by regulators is essential to make sure that the spirit of laws and regulations are carried out in changing market circumstances. Finally, the day-to-day functioning of the market is carried out by a network of trusted intermediaries (exchanges, clearinghouses, and licensed broker/dealers) and trusted third parties (rating agencies, public accountants, etc.). While these intermediaries and third parties are private institutions, they have a quasi-legal role and have a degree of governmental sanction and oversight. We expect to see a similar framework evolve to support incentive-based cyber trust, perhaps even drawing on the existing framework for financial markets.

In comparison to the legal, regulatory, and institutional framework required by the other approaches, the "free market framework" is more efficient and more agile to adapt to changing circumstances. It scales better, both in size and across geographic and jurisdictional boundaries. Finally, it is much more likely to foster innovation and avoid unproductive stakeholder conflict.

5. EXAMPLES

To give you a practical understanding of the innovations that might be possible, we offer five illustrative examples. These are illustrative examples only, and not meant to represent well-developed theories or provably viable projects. To keep the discussion short, we won't explore each example in detail, provide full references, or evaluate feasibility. Consider these examples as food for thought and jumping-off points for other ideas.

5.1. Near-term examples

Here are several relatively simple, limited examples of how incentive-based cyber trust can work in practice. These examples either exist to today or can be implemented with current technology and research knowledge. For each, we suggest improvements that would increase their effectiveness in terms of incentives.

1. **Supply chain contingent payments** – it's common practice for supply chain partners (incl. outsourcing) to have contracts that govern their relationship and transactions, including clauses for information security practices and requirements. These clauses usually define mandates and, sometimes, penalties. While incentive contracts have been used in some cases to manage supply chain risk [124] [125], especially to build trust and commitment [126]. However, it is generally not used to manage cyber risk specifically. Even so, it should be possible to define contingent payment(s) tied to specific information security goals, measured by existing operational metrics or scorecards [127]. The contingent payment amounts would be negotiated. While these instruments would provide relatively crude incentives, it could be more efficient than a purely mandates + penalties approach, especially if it promotes creative solutions and information sharing to reduce mutual risks.
2. **Identity theft insurance** – in the US, several companies provide identity theft insurance. While many policies cover both credit losses and lost wages, this insurance doesn't cover the largest potential cost – destruction of consumer's credit rating [128]. Furthermore, premiums for identity theft do not reflect the relative risk of policy holders. Identity theft insurance could be a more effective cyber trust incentive instrument if even simple methods were used to value expected drop in credit rating vs. income level, and also rating the risk exposure and reduction practices of policy holders. This would provide risk pricing information to consumers and might improve their risk mitigation behavior.
3. **Vulnerability bounties** – several organizations offer bounties (i.e. contingent payments) to independent security researchers if they submit "zero day" vulnerabilities (i.e. unpublished vulnerabilities that have no patch or fix available) [129] [92] [93]. Obviously, the intent is to create incentives for independent security

researchers to find and submit vulnerability information that they would not share otherwise. If the bounty transactions were made public and framed a risk management context, it has the potential to serve as an additional incentive for software vendors to minimize and quickly eliminate vulnerabilities.

4. **Open source digital rights management** – From the viewpoint of cyber trust incentives, DRM has been hampered by political problems (e.g. abuse of monopoly power and burden shifting) caused by closed-source, proprietary DRM methods used by large vendors. If DRM is ever going to include or fit into cyber trust incentive systems that protect all stakeholders, not just the content owner, then DRM needs to be open to examination, at least, or preferably open source. Sun Microsystems has launched an open source digital rights management (DRM) initiative called "Open Media Commons" [130] [131]. Other open source DRM is also available [132], along with an open rights specification language [133]. Open DRM has the potential to be more effective in honoring consumer privacy rights, fair use, freedom of speech, and alternative rights schemes such as Creative Commons [134]. Even arch-critics of DRM have commented that open source DRM is significantly better for social welfare than its closed, proprietary alternatives [135] [136]. With open DRM, it would be comparatively easy to define and build extensions that provide cyber trust incentive payments or other benefits to stakeholders other than the content owner. This could lead to the use of DRM-like technology to help manage cyber trust in contexts other than entertainment media.
5. **Content micropayments that include cyber insurance** – with the dramatic market success of ring tones for mobile phones and download music services like iPod/iMusic, micropayment schemes for content have become very well established [137]. Another example is FaceBridge, a start-up company that is developing a general-purpose micropayment system for voice over IP (VoIP), instant messaging (IM), and video IM. They call it "pay-per-view for the masses", since anyone can charge anyone else to view content [138]. With any of these micropayment systems, it should be possible to add "micro-insurance" payments on top of the content payment, even to a third-party insurance provider, where the level of payment is determined by the relative risk the transactions and parties (malware, fraud, piracy, etc.). Such a system could start with a relatively simple risk scoring method and evolve to more sophisticated methods. These micro-insurance payments (including rebates) could be tied to information sharing by the parties, e.g. reputation ratings, post-transaction evaluations, etc. Overall, there could be systemic benefits to such a micro-insurance scheme, since it could help prevent or limit fraud in the micropayment systems themselves, since the insurance providers provide a cross-check on user behavior.

The next set of examples are considerably more complex and raise substantial research questions, but offer more substantial benefits.

5.2. Risk-sharing instrument for ICT products and services

Problem: Information and communication technology (ICT) buyers often feel as though both operating costs and risk of cyber trust are being dumped on them by vendors through license contracts, service contracts, pricing, and vendor testing and patch release practices (See Section 5.4). For example, one industry group estimates that the US financial services industry spending on vulnerability and patch management approaches $1B per year [139]. Furthermore, no party in the value chain is disclosing or sharing enough information about vulnerabilities in ICT products, which essentially means that all parties are making decisions in relative darkness. What's missing is compelling incentives for the ICT vendors and buyers to share cyber trust information and work together to implement cost-effective solutions.

It's widely recognized that emergent forms of value for ICT in use (e.g. quality, security, and availability) are jointly created by ICT vendors and their customers. Therefore, cyber trust outcomes should be managed as a joint responsibility. However, current payment and relationship structures don't reflect these facts. No one has figured out how to charge more for higher quality or more secure software due to the "lemon's market" effect (i.e. systemic under-pricing in the used car market due to information asymmetries about quality and post-purchase costs). [140]

Solution: a "risk/reward sharing instrument" between IT vendors and their customers that effectively creates risk-adjusted pricing and gain sharing, plus incentives for information disclosure and learning [141] [142]. Here's how it might work:

- The instrument(s) would be some form of forward contract on predefined cash flows from both ICT vendors and customers, approximating a portion of the self-insurance pool for each party associated with their joint cyber trust risks.

- The cash flows would be calculated through activity-driven models using observable quality, reliability, availability, and security metrics, similar to those that are the foundation of Service Level Agreements (SLAs) [143].
- Both vendors and customers would regularly feed metrics information to a trusted third party, who would use simulation models to estimate the expected cash flows and then publish the results. Periodic audits and comparison with public financial statements would be used to validate the output of the activity-driven cash flow models.
- The cost of externalities (i.e. systemic risk) could be included in the models in a variety of forms.
- Based on simulated performance driven by actual operational results, vendors and customers either share the gain (better-than-expected), or loss (worse-than-expected), according to pre-agreed formulas or triggers. (Similar approaches in financial risk management are called "mark-to-model" and "mark-to-future". [144])
- Because they represent cash flows, these instruments could be bundled, repackaged, sold on secondary markets, or tied to subordinated debt to provide liquidity and/or market prices for risk.
- The resulting risk prices could serve the same incentive and signaling effect as insurance premiums for traditional property/casualty.

This solution could make a revenue contribution to ICT vendors because any time you can optimize the pricing/packaging/placement of a product or service to better fit what the customers really want, you have the potential to increase customer satisfaction, market share, "share of wallet", or to open up new segments that were not previously economical.

In each organization, the risk management department or function would need to take the lead in order to quantify the risks and to create the appropriate instruments, contracts, or policies to control them and/or hedge. No one else in the organization would have the skills or tools in modeling, analysis, and decision theory to handle it with sufficient credibility. It also would require close collaboration with other functions, including product marketing, legal, product development, finance, and customer support.

5.3. Real-time cyber risk dashboard for end users and consumers

Problem: Consumers and individual ICT users generally do not have sufficient understanding or enough information to make good risk/reward decisions regarding cyber trust. This is true not only for major decisions (e.g. purchase, configuration, update, or upgrade) but also for moment-by-moment usage decisions (e.g. visit a web site, enter personal information, use a public WiFi access point, use peer-to-peer file sharing, etc.). As a result, consumers and individual ICT users are both too cautious and too lax in their practices. At best, this leads consumers to worry and feel discomfort; at worst, loss of tangible or reputation. It also creates significant external costs for other individuals and institutions.

Today, some information to guide the consumer comes from screen icons (e.g. the "lock" icon on Internet Explorer), cryptic pop-up messages, help files, procedure manuals (rarely used), or from a human helper (if available, knowledgeable, and not too much of a hassle to deal with).

Solution: a dashboard or other animated display that provides risk feedback in real-time as the consumer or individual is making use of the ICT devices and services. Microsoft's Internet Explorer (IE) 7 comes with a simplified version of this solution, to warn users about known phishing web sites. Also, Symantec has released a free to download Symantec Internet Threat Meter, based on Yahoo! widgets platform [145]. It displays a qualitative risk index rates the four main online activities, including e-mail, web activities, instant messaging and file sharing on a low, medium or high risk level based on general conditions on the internet, but not on a particular user's system or related to their specific activities.

What we are suggesting is much more complete and compelling for the consumer.

Here's how it might work:

- It would need to be fed by a knowledge base of considerable depth and sophistication, preferably pooling the knowledge of many users in similar circumstances. Peer-to-peer data and knowledge sharing models could be appealing, with appropriate mechanisms for preserving anonymity and protection against gaming the system.
- Sophisticated modeling would be required to characterize the user's configuration, assets at risk, normal and abnormal activity patterns, risk tolerance, and to map these factors to threats. However, considerable modeling and data complexity can be avoided through abstraction, pattern recognition, and inferential reasoning.
- Prediction markets for estimating or forecasting key parameters could be useful. Participants could include ICT vendors, security and privacy experts, risk management professionals, and even (by proxy) consumers themselves.
- The most important information to give the consumer/user is relative expected value changes for alternative courses of action (e.g. visit the site vs. not). While it is tempting to put this into a rigorous decision-theoretic framework using money values, that may not be necessary or even

the most useful way to model or convey the information.

- Whatever information is chosen for display, it's critical that it is displayed in a meaningful, compelling, and comfortable way. Perhaps there is some middle ground between the static or animated icons now used on browsers and the animated cartoon Office Assistant by Microsoft, which was engaging but entirely uninformative.

This solution might be offered as an independent product or service, or it might be bundled with existing or new products or services, which might speed adoption and enhance the value proposition for both consumers and vendors. For example, if this solution were linked with a consumer risk sharing pool, then it might be possible to display their real-time "insurance premium", "coverage limit", or other related self-insurance or mutual assurance value (either monetary or in-kind value).

Clearly, this solution would require many theoretical and practical innovations, including risk modeling, data sharing and aggregation, and risk communications.

5.4. Enterprise total cost of (in)security

Problem: One of the main challenges facing information technology (IT) managers and business executives is how to map security metrics and performance to business metrics and performance [8]. This is necessary to align business goals and investments with security requirements, and to balance risks against costs and rewards. Because the benefits of security are the avoidance of uncertain losses, applying traditional cash flow return on investment (ROI) techniques would be inappropriate and misleading. Furthermore, the domain is rife with "unruly uncertainty" (ambiguity, incomplete information, contradictory information, intractability, unknown-unknowns, etc. [16] [146] [147] [148] [149]) which make it difficult or impossible to reliably estimate annualized loss expectation (ALE) or other probabilistic estimates of expected losses for given incident types.

Solution: managerial accounting methods and decision support tools to measure the Total Cost of Security (or Insecurity). Here's how it might work:

- Divide security-related or cyber trust costs into three categories: "Budgeted", "Self-insured", and "Catastrophic" (Figure 1). Basically, this approach divides the aggregate cost probability distribution into three sections. The fat part of the curve near the mean is "budgeted". The tail section up to some threshold (95%, 99%) is "self-insured". The very far end of the tail is "catastrophic". Therefore, any given incident type, vulnerability, or threat could contribute costs into any or all of these categories.

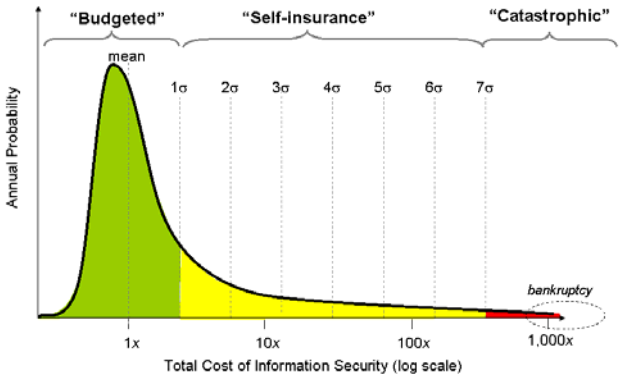

Figure 1. Idealized Probability Distribution for an Enterprise's Total Cost of (In)security

  - "Budgeted costs" are defined to be costs that are predictable and likely within the budget year. This includes all direct spending on security, plus indirect costs, plus the expected value of all high frequency losses and some small mix of lower frequency losses. It also includes the opportunity costs – business activities that are prevented or inhibited by security.
  - "Self-insured costs" are less predictable and/or much lower probability within the budget year. Loss magnitudes are potentially big enough to bust the budget (i.e. material to quarterly earnings statements) and even threaten the firm's credit rating, but not necessarily threaten firm survival.
  - "Catastrophic Costs" are very unlikely and/or very unpredictable, but could threaten firm survival or even more widespread systemic losses.
- Cost models would be built for each category, drawing on operational security metrics, business process metrics, and estimates of asset value and other values at risk. But the models for each category will be very different.
  - Budgeted costs would be modeled using fairly conventional cost-driver models (i.e. linear relationships between operational metrics and indirect or overhead costs, etc.).
  - Self-insured costs would be modeled using rank order or order-of-magnitude approaches, possibly combining stochastic methods with inferential reasoning (see Section 5.5, below).

- Catastrophic costs would be modeled using scenario analysis and ordinal or nominal scales. Here, the precision of cost estimate is much less important than it's the qualitative value to guide strategy and business continuity planning, for example.

This solution would work for any type of security risk or, more broadly, cyber risk. If the loss distribution estimate happens to be normal distribution with relatively modest variance, then it would all fall into the "budgeted" category, and thus could be managed using traditional budget and cash flow methods. On the other hand, if the loss distribution has a "fat tail", then the three-part approach becomes very useful to distinguish between what we know with confidence and what we know with less confidence or don't know at all.

This solution makes the most of existing information, aligns with decision-making processes, and avoids the problem of conflating reliable and unreliable estimates. It requires innovations from Enterprise Risk Management, Activity-based Costing, and qualitative reasoning. The approach is roughly analogous to the Total Cost of Quality concept that helped motivate the Total Quality Management movement [150] [151]. In addition to helping with security cost and performance management, this approach highlights the importance of organization learning and discovery.

Another advantage of this method is that it is compatible with existing methods for enterprise investment and performance management, including "Risk-adjusted Return on Capital" (RAROC) [152] [153] in financial services and "Economic Value-added" (EVA) [154] across various industries. In essence, "self-insurance" adds to the capital required by a project or business unit. Higher levels of cyber risk mean a larger "self-insurance" pool is required, which lowers return on capital, and vice versa [155]

It may be possible to standardize these methods with industries and organization types to allow, for the first time, meaningful aggregation of cyber trust cost information to guide government policy and vendor product development decisions. It would also allow meaningful public disclosure of cyber trust risks and risk tolerance in stakeholder reports and regulatory filings.

5.5. Incentive funds for vulnerability research and resolution

Problem: The current software development and release process for commercial vendors is sometimes derisively called "patch and pray", meaning products are released with known or unknown vulnerabilities, which are then discovered in the marketplace, prompting vendors to create "security patches" and "pray" that they have covered the vulnerabilities. This cycle puts the customer into the quality control loop. One observer writes:

> "Software companies with an engrained culture and processes to get it "mostly right" ship code with security vulnerabilities (often unwittingly because they did not adequately inspect the emergent property or were lulled into a false sense of security due to some high profile security feature).
>
> Then an adversary finds and exploits the vulnerability. For commercial software companies, these are often researchers who do not care if the software is mostly correct, all they need to find is one hole and they publish a high profile report. That gets reported in the news, the software company rushes to fix that problem and rapidly ships out another patch, and so on, and so on. In the end the customers are frustrated about constantly being rolled between the rock and hard place of either patching their production systems or leaving them vulnerable to what is by then a widely known security bug. […]
>
> All too often it is only after we build a piece of software that we (or our users) can adequately (a relative term) say what they actually wanted. […] it is fundamentally driven by the fact that most complex software (particularly application software) is automating some activity or process which is itself ill defined. […]
>
> Since the major issue with most systems is definition of precisely what it must do, and that is often times impossible without actually building it first, when it is played out in a competitive environment, the company that ships something first is at an extraordinary advantage. For they are the ones who start the iterative process of perfecting the quality by perfecting the specification. This has been institutionalized in the familiar Alpha and Beta version or the infamous 1.0 of any new software product. Software is deployed to users long before it is completed in order to improve the quality (from a definition point of view) and manor points have been given to the firms that get it in these user's hand first. Well in the process of doing that, these users (Alpha and Beta testers along with 1.X users) also tend to catch "quality problems" with the software and they tend to report them as bugs. Today most software packages facilitate the reporting of these bugs as soon as they are encountered (Dr. Watson) and the user continues to play a critical role in the overall quality process." [156]

Thus, customers and other parties external to the software vendor contribute value to software vendors by finding, researching, and reporting vulnerabilities. One of the incentive problems related to this is how and whether vulnerability research and reporting is compensated, by whom, and by how much.

A related problem in the lifecycle is how fast and how well the software patch is developed, tested, and released. Currently, vendors have complete discretion and do not always act in ways that benefit customers. Evidence is the significant cost in large corporations associated with testing patches before distributing and installing them, both direct cost and the indirect cost of leaving systems vulnerable to known exploits.

Several innovative solutions to the problem of vulnerability research and resolution have been offered and tried, including vulnerability auctions and bounties (See item 3, in Section 5.1). To date, none of these innovative solutions have been adopted on a wide spread basis. The reasons vary, but one common factor is lack of alignment between the economic and political interests of the various stakeholders.

Solution: application of the "Street Performer Protocol" and completion bonds, or variations. The Street Performer Protocol was proposed first by John Kelsey and Bruce Schnier in 1998 [157]. Briefly, people (customers, vendors) could place donations to support vulnerability research in escrow, to be released to an author in the event that the promised work (vulnerability discovery and/or resolution) is put in the public domain (or released and verified). This mechanism requires trusted third parties to act as escrow agents and to possibly validate successful completion. Drawing on this idea and also "social policy bonds" [158], Chris Rasch proposed a "Wall Street Performer Protocol" (software completion bonds) as a method to fund open source software development [159]. Here is Chris' summary:

> "A software completion bond is a promise to pay the bond owner the face value of the bond when anyone, anywhere in the world, completes software that meets the bond specifications. A software completion bond is created when an individual who wants to fund the development of an open source software package backs a bond by agreeing to place the face value of the bond in an interest bearing escrow account. The 'bond backer' agrees to accept the judgment of the 'bond judge(s)', who are appointed at the time of the bond's creation. The 'bond backer' agrees to pay off the bond when the 'bond judge(s)' determine that the specs have been met. A bond may or may not have a time limit associated with it, depending on the desire of the bond backer." [159]

While these solutions were proposed to fund public domain works, they can be adapted and applied to vulnerability research and resolution. Because they provide funding up front, the economic incentives for performing research and/or resolution tasks becomes more visible. Thanks to the "donation" model, any and all stakeholders can contribute, even acting as proxies for other stakeholders (e.g. consumers). The assurance procedures would help ensure that the money went primarily to productive activity, i.e. fruitful vulnerability testing and resolution, even though that activity is somewhat speculative. It can be tied to reputation systems where vulnerability researchers earn higher (or minimum) payouts as their reputation grows. Of course, many complex problems remain in defining the details of this approach, including how to resolve competing claims for finding a particular vulnerability.

5.6. Simulation games and simulated markets for cyber risk valuation

Problem: From an economic point of view, one of the main obstacles to any incentive-base approach to cyber trust is how to value (monetize) the associated risks. As we mentioned above, the most sophisticated approach draws on actuarial methods from the insurance industry to define a "risk premium" associated with forecasted expected losses. If large quantities of robust data were available, this approach might be the complete solution. However, given the lack of data and the rapid environmental changes in cyber trust, it's not likely that any approach based solely on historical data analysis will ever solve the valuation problem.

Solution: large-scale simulation games and simulated markets. These and other tools from experimental economics [160] could be used to generate cyber trust valuation data. While many approaches are possible, we will discuss a variant of scenario analysis [161], which is well established in the fields of disaster planning, and policy analysis [162]. Think of it as a two-stage process. First, plausible simulation models would be built using available information on cause-effect relationships. Second,, the simulations would be run across many scenarios and parameter values in Monte Carlo fashion. Strictly speaking, this would not be a forecast or prediction of future events, but instead an exploration of the space of possibilities. It is possible to make inferences and preferential decisions using scenario analysis, even when the outcomes are qualitative. However, it may be possible to create quantified cyber trust simulations drawing on real-world parameters and ratings, with the outputs serving as guidelines or benchmarks for real economic valuations. The key to this whole approach would be providing rigorous evaluation of the plausibility of the simulations. This could be done through formal methods of mathematical logic ("reasoning about uncertainty" [163]) or by various social methods such as peer review and competitions.

A related approach is to create simulated markets. Prediction markets [164] can be used to pool the "wisdom of crowds" to make predictions about specific events. In the arena of cyber trust, prediction markets might be used provide continuously updated estimates of the likelihood and severity of various types of breach events, for example. Or perhaps they could be used to predict

relative values or rates. It might also be used on a more fine-grained level, e.g. to estimate the number of published vulnerabilities for future software releases. Simulated markets can also be used to "securitize" the value of non-traded or intangible assets. This would be particularly useful in conjunction with the simulated games, mentioned above.

Another angle is to use massively multiplayer online role-playing games (MMORGs) as experimental environments. While many MMORGs might have some suitable characteristics, *Second Life* [165] [166] is currently best situated for incentive-based cyber trust experiments. Nearly everything in the game is created by players, facilitated by a sanctioned economy. Unlike nearly ever other MMORG, *Second Life* players retain real-world intellectual property rights. There are also features that allow broadcast or use copyrighted material (e.g. music, video, web pages, logos, etc.). Both *Second Life* members and real-life stakeholders face a broad range of cyber trust challenges – intellectual property [167], digital rights [168], privacy [169] and information security [170] [171]. The strategy of Linden Labs, host of Second Life, is to mobilize free market forces to stimulate innovative solutions to these challenges:

> "Virtual works will, out of necessity, pioneer solutions to virtual and digital property long before the real world does. […] By making the right intellectual property decisions, virtual worlds have the potential to be far more innovative than the real world, while still providing sufficient incentive for creators." [172]

Second Life has a significant number of educational and research members [173], but none so far (that we know of) focused on cyber trust research.

While not as compelling as real-life data, simulated games and markets may provide the best avenue to forward-looking risk valuation in the fast-changing cyber trust environment.

6. INITIATIVE DESIGN

To stimulate discussion and as a *prima facie* case for feasibility, we briefly sketch how an initiative might be designed and managed, given the institutional landscape for cyber trust research and development. (We survey the cyber trust R&D landscape elsewhere [174], showing how an Initiative would fit in and interact with existing institutions and stakeholders.)

As an organized set of activities and resources, the main chore of the Initiative will be to "connect the dots" with existing institutions, organizations, disciplines, and resources. Thus, there is no need for a large organization or staff. Furthermore, we do not see the need to have a central institution to serve as a source of funding or other financial/legal support. These considerations lead to the following design elements:

- **Virtual organization** – modeled on any one of several modern consortia and social networks. This includes all the internet-based collaboration methods, but also the governance, involvement, and communication practices that have succeeded so well in the open source community (just one example of many).
- **Communities of practice** [175] – to facilitate collaboration and cooperation on many levels, with very diverse and geographically dispersed participants. This requirement calls for organization capabilities to support ad hoc collaboration and informal group formation.
- **Respected sponsorship** – The sponsors would provide a "home" for the Initiative, at least until it establishes its own reputation and resource base. Credibility and confidence in the Initiative would be greatly enhanced if it were sponsored by one or several respected organizations that have a track record of success in the general area of cyber trust, especially in bridging between academia and industry and also public policy and private interests. Finally, the sponsors should be well regarded as "honest brokers", entrepreneurial innovators (or perhaps practical futurists), and, last but not least, globally oriented.
- **Attractor for funding and resources** – While not a funding institution itself, the Initiative should stimulate increase funding for cyber trust R&D, both in academia and in industry. An important goal will be to increase R&D funding from sources that are not currently investing significantly in incentive-based cyber trust, including large firms in ICT, financial services, health care, and information services. Another goal is to attract more academic and industry professionals to the arena of cyber trust, especially from backgrounds that bridge technical and non-technical disciplines.
- **Nurturing environment for radical innovations** – between first concept and widespread adoption, radical innovations require special care and feeding [176] [177]. This is especially true for innovations or theories that don't have a natural home in one organization, profession or academic discipline (e.g. complexity science [178]). At the same time, there needs to be a vetting procedure so that truly promising innovations get ever-more support and to filter out unsound or misguided efforts, and to guide them toward successful implementation [179]
- **Results- and action-oriented** – In other words, the Initiative needs to be something more than a debating society or an interest group. While this is

easy to say, it's hard to do in an otherwise loose environment. Results incentives might be useful, including cultural norms, financial prizes, and professional awards. Showing useful results early will greatly help the Initiative get off the ground and gain respect. The first "deliverable" of the Initiative will probably be a research agenda with targets and milestones.

- **Catalytic and synergistic** – To have any meaning as an Initiative, some activities must be performed beyond merely connecting existing people and resources. Catalyst activities could include "Grand Challenge" prize contests, prestigious events or publications, or even informal/social incentives. Synergy, in this context, literally means organizing collaborative projects between people and organizations that previously worked separately.
- **Non-partisan but active in public policy** – cyber trust is a hot political topic, both in government and industry. Possible legislative, regulatory, and court actions have led to adversarial (partisan) lobbying by various interest groups. This Initiative should not be used by any one interest group to further their agenda at the expense of others. However, the Initiative has much to offer the policy debate, including new "win-win" solutions to current "win-lose" problems, and also meaningful analysis of factual data or realistic simulations.
- **Internationally oriented** – The scientists and engineering working on computer security have collaborated internationally for many years. The same cannot be said regarding economic and sociological aspects of cyber trust until very recently. Of course, the cultural, legal, and economic landscape is dramatically different across regions and countries, which makes it much harder and more expensive to do truly international research. The Initiative could significantly increase the level and quality of international research and research collaboration, especially by drawing in regions that have not been involved much to date (e.g. Asia, Africa, Latin America).

Of course, this list of elements is only a start. Many details remain to be defined.

7. RESEARCH QUESTIONS

The proposed Initiative encompasses many important and difficult research questions. While there are near-term product/service development opportunities related to incentive-based cyber trust, the main reason we are proposing an Initiative is that there are so many central research questions that must be resolved first. Here is a starter list to stimulate discussion:

1. **Theory**
   a. Is it theoretically possible to model cyber trust risks and incentives in a unified, forward-looking valuation framework? What are the fundamental limits [17] [180] [181]?
   b. If analytic, quantitative models are not feasible, is it possible to devise coarse-grained or qualitative models that are robust and usable in practice (e.g. rating or ranking schemes) as the basis for incentive instruments?
2. **Usability**
   a. How does cyber trust usability (generally) affect and influence other cyber trust incentives (e.g. remunerative incentives)?
   b. How can personal incentives be created through product or service design, or through ancillary services?
3. **Risk information systems**
   a. How can we gather more useful and insightful risk information (incidents, losses, spending, etc.) to provide a sufficient data foundation for risk and incentive modeling? Specifically, there is a need to improve on the CSI-FBI survey to sample a much larger population in a statistically reliable way in order to estimate the likelihood and severity of low frequency-high loss events. Another crucial need is for transnational risk information.
   b. How can decision-makers cope with all relevant types of uncertainty and ignorance associated with cyber trust risk information [146] [147]? Can we usefully and reliably model risk in a forward-looking fashion in the absence of traditional actuarial databases? Can we leverage methods from artificial intelligence, automated reasoning, mathematical logic, or cognitive science?
   c. What is the cause-effect relationship between operational cyber trust metrics and stakeholder value? How can we map existing assessments, audits, and metrics to a risk modeling framework? We need to have more general and robust methods to determine the relative risk associated with higher or lower scores on assessments.
   d. How can we model the cash flow implications of cyber trust in a way that maps to existing accounting and budgeting frameworks? Can we leverage methods in other fields such as financial engineering or computational organization theory?

e. What sort of incentives and protections can be created to encourage organizations to collect and share cyber trust information?
f. How can cyber trust risk information be communicated in the context of the upside of risk taking behavior, so that decision-makers can actively balance those factors?
g. How can we protect incentive-based cyber trust systems from manipulation, corruption, abuse, or security breaches? How can they be made robust?

4. Risk communication

a. How can cyber trust awareness training be designed to include incentives and incentive instruments for participants, e.g. to help them make better risk management decisions?
b. Is it possible to design cyber trust risk "dashboards" so that people at all levels of organizations have real-time and context specific information to guide actions and decisions?
c. How can we measure risk and impact when the value at risk is not purely quantitative or monetary (e.g. trust, confidence, reputation, etc.)?
d. How can we create personal incentives for disclosing cyber trust information?
e. Can we use modern graphics and animation methods to communicate complex risk dynamics in a way that ordinary people can understand?

5. Social knowledge

a. Can we use simulations, prediction markets, or other social knowledge methods to fill in the blanks in our empirical data?
b. How can we use existing and new communities of practice [182] to create generate useful knowledge to support incentive-based cyber trust? (Examples of such communities today include vulnerability researchers, open source developers/testers, privacy activists and watchdogs, and professional/industry associations such as the Software Industry Association.) Can we leverage those communities of practice to create "open" or "democratic innovation networks" [183]? How can the participants share in the economic gains of such networks?

6. Markets

a. Can we create new markets (goods, services, or financial assets) that support incentive-based cyber trust? Ideas proposed to date include "cap and trade" markets and "bug auctions". We listed other ideas and approaches in Section 4.5, above.
b. If such markets are created, how can they aid in price discovery, to provide funding or financing, or to support incentive instruments?
c. Can simulated or artificial markets be used to provide reliable, useful forward-looking valuations that can serve as the basis for real-world economic decisions and commitments (e.g. incentive instruments)?

7. Incentive instruments

a. Can we extend the existing types of cyber insurance from commercial carriers so that they are more widely applicable, more efficient, and easier to use in risk management?
b. Is it possible to define general-purpose and standardized risk-sharing contracts for trading partners to serve as mutual incentives for cyber trust? Are these risk-sharing contracts more efficient and effective than mandates-based and penalty-based approaches?
c. Is it possible to define a framework for self-insurance so that organizations can account for cyber trust risk that they retain within existing accounting methods?
d. Is it possible to define risk pools or other quasi-insurance schemes to provide risk pricing within social and economic networks?
e. Can methods from digital rights management be adapted to other aspects of cyber trust, including privacy rights?

8. Enabling technology

a. How can support for incentive-based cyber trust mechanisms be embedded in ICT systems? This is especially needed in SaaS, "cloud computing", information services, and mobile computing.
b. How can cyber trust risk information be used by ICT systems to make better automated decisions (e.g. reconfiguration, recovery) [184]?
c. How can ICT systems communicate cyber trust information to minimize user confusion?

9. Supporting legal, regulatory, and institutional framework

a. How can existing information standards be used to support incentive-based cyber trust? Examples include e-commerce standards, software quality standards, security/privacy standards, web services standards, and

knowledge management standards. Are new standards needed?

b. How do existing and emerging laws and regulations support or not support incentive-based cyber trust? This includes copyright, patents, privacy, security, digital rights, product liability, anti-trust, trade secrets, and so on. What new laws or regulations are needed? How would these be rationalized across jurisdictions?

c. What existing or new trusted third party institutions are needed to facilitate incentive-based cyber trust?

d. What are the "power politics" of cyber trust [185]? What are the interest groups, factions, alliances, conflicts, and battlegrounds? How do these "power politics" inhibit or support the development of incentive-based cyber trust? What are the implications on the legal, regulatory, and institutional framework?

8. GETTING STARTED

Starting this Initiative won't be easy but there are many positive forces and developments to build on. At a policy level, there is strong support for some form of incentive-based cyber trust. There have been many prestigious panels and study groups that made such recommendations, including the Computer Research Association [3], the US Interagency Working Group on Cyber Security and Information Assurance [186], the US President's Information Technology Advisory Committee [187], and the international 2005 Rueschlikon Conference on Information Policy [188]. The key challenge now is to convert this policy-level support into meaningful action. (This is also being studied by the Committee on Improving Cybersecurity Research in the United States [189], as mandated by Congress by Cyber Security Research and Development Act of 2002. Their final report has not yet been published.)

Most important will be to get sponsorship and support from one or more industries that have the greatest and most pressing needs. Leading candidates include:

- **Financial services –** there has been a revolution in quantitative risk management in the financial services industry, culminating in the Basel II Accord to promote stability in the financial system through, among other things, market discipline (i.e. incentives). This has led most large banks and insurance companies to take a more comprehensive approach to risk, including developing sophisticated models of operational risk, which includes cyber risk. At the very least, this provides some of the prerequisite skills, knowledge, and management awareness to begin to tackle the sort of incentive-based approaches put forward in this paper.
- **Health care –** Breakthrough innovations in health care service delivery will depend heavily on sophisticated security and privacy capabilities. "Electronic health records have not yet become universal, so that when a patient moves from primary care doctor to specialist to ED to hospital, each health care professional the patient sees must start from scratch in diagnosing the patient's condition and treating it. Beyond this, isolation of the components of our healthcare system from each other. People visit multiple healthcare providers […] and providers often do not know who else is providing care, what medications have been prescribed, or what past tests have revealed. […] Critical information is often not there when it is needed so doctors can make sound judgments. The result is money being wasted on duplicate tests, delays in treatment while waiting on record transfers, and, sometimes, errors in diagnosis and treatment." [190]
- **Media and Entertainment –** traditional media and entertainment companies have been hit on the top line (revenue) and bottom line (profit) by the invasion of digital technologies that make it easy to produce, copy, transmit, and repurpose information and creative works. In addition, the democratizing force of technology is pushing these industry transformations into the developing world, as well, so this is a global issue [191]. While digital rights management is in the forefront in the minds of industry executives, the Sony BMG Music case is just one example of how information security, privacy, and IP protection all intertwine in this industry. Unfortunately, much of the energy from the industry has been invested in penalty-based, political, and technological approaches, which often benefit one or more stakeholder groups at the expense of others. Incentive-based cyber trust could radically improve the economics of media and entertainment with greater overall social welfare compared to the other approaches. One reason this may be true is that it is in line with one major media/entertainment trend – "consumers as content producers" [192]. This tilts the market forces in favor of a widely distributed gain-sharing and incentive system rather than tightly controlled and intrusive digital rights systems.
- **Software and Information Services –** there are several emerging models of software and information services that introduce new cyber trust challenges, including Sofware as a Service (SaaS)

and Service Grids. "Software as a Service is a software application delivery model where a software vendor develops a web-native software application and hosts and operates (either independently or through a third-party) the application for use by its customers over the Internet. […] SaaS was originally considered a potential security and operational risk. Many businesses wish to keep their information technology operations under internal control. However, there is a counter-argument that the professionals operating SaaS applications may have much better security and redundancy tools available to them, and therefore the level of service may be superior in many cases." [193] Service Grid is a service model similar to SaaS, but where SaaS model is one (vendor) to many, the Service Grid model is many-to-many using loose networks of cooperating web services [194]. Cyber trust in service grids have been debated recently [195]. Beyond the technical aspects, it's clear that trust and reputation management needs to be a core function: "The service grid is an excellent nexus for monitoring and evolving the *reputation* of various application services of the service grid." [emphasis added][195] Historically, software and information service vendors have focused on IP protection and digital rights (license management), and the cyber trust challenge for their customers was information security and data protection. With SaaS and Service Grids, these boundaries and responsibilities have become blurred, and there exists no good way today to mandate cyber trust for computing and data that's "in the cloud"[2] [196] [197]). Incentive-based cyber trust could greatly expand and lubricate the market for SaaS and other emerging software and information service models.

- **Critical infrastructure** – industries that are deemed "critical" include electricity and energy distribution, transportation, public health, telecommunications, transportation, and banking. While these industries have a long tradition of reliability engineering, disaster planning, etc., they are becoming more interdependent with each other and more dependent on information technology, which means they are more concerned about cyber trust issues. Facing threats such as major accidents, natural disaster, hackers, and cyber terror, it's essential to avoid or recover quickly from a service interruption. The key challenge is "how to steer multi-actor decision making toward an adequate performance of the integrated system with respect to long-term public interests" [198]. Incentive-based cyber trust could be very useful to help manage and protect the ICT systems that control these critical infrastructures, especially throughout supply chains and outsource relationships.
- **Electronics Supply Chain** – several trends have caused cyber trust issues to become more significant in the electronics supply chain. The electronics and electronic equipment industries have always had significant concerns about intellectual property (IP). What's new in the last several years is that more of the IP has become "soft" – i.e. packaged and distributed in digital form, which is then embedded in chips and equipment. This increases the importance and complexity of IP protection and digital rights issues [199] [200]. Furthermore it introduces information security concerns since the digital IP needs to be protected from malicious intrusions as it passes through the supply chain and also from run-of-the-mill security vulnerabilities. Finally, the increasing complexity of the supply chain itself means that information systems used that manage the supply chain introduce complex interdependencies and systemic risks [201] [202] Incentive-based cyber trust, as part of a holistic supply chain risk management process, could align incentives for supply chain actors to increase resiliency, even in the face of unforeseen scenarios.
- **National security** – last but not least, the national security agencies of all industrialized countries have long invested in advanced information security technologies [36]. However, with the expansion and proliferation of ICT and public networks, achieving national security goals also requires reliance on commercial off-the-shelf (COTS) ICT products and services, along with the critical infrastructure industries mentioned above. Disaster management is another area where ICT has also become critical [203]. This means that national security agencies now have to contend with all the same cyber trust concerns that face the private market institutions. [204] . Conversely, there are many cases where commercial and

[2] "Cloud Computing — (Also called distributed processing, Grid Computing, mesh networks) where "clouds" of computers are deployed to provide a virtual computing environment to accomplish a given task by distributing processing load and data. Cloud Computing brings servers on-line as needed, and the end user does not know where the data resides or executes at any point. In some cases, the application runs on a combination of servers and on the user's PC. Server clouds can reside physically in large facilities controlled by one organization or they can also reside all over the Internet. Because resizable computing capacity is based on virtual servers the *data owner does not really know where his programs and data reside physically*." [emphasis added] [197]

private cyber trust impacts or conflicts with the national security interests [205] [206] [207].

Individual companies in these industries might have characteristics that could inhibit their commitment or adoption of incentive-based cyber trust, e.g. include lack of resources, internal politics, and unwillingness to adopt radically new methods. Therefore, the Initiative will require an active recruiting effort to identify lead sponsors and early adopters.

Another important start-up tactic will be to build on existing collaborative research and development efforts. Just one of many examples is the Workshop on the Economics of Information Security (WEIS) [208], which is holding its sixth annual event in June, 2007. WEIS draws over 100 leading academics and industry practitioners to review the best research and to share the latest ideas. The proposed Initiative would not supplant WEIS or similar workshops, conferences, or collaborations. Instead it would build on it and amplify its effectiveness by linking with other efforts in the cyber trust R&D

9. CLOSING REMARKS

The economic and social problems of cyber trust are difficult and complex. The Sony BMG Music Entertainment case discussed in the Introduction illustrates the complexity of the problem and points to the importance of incentives. Sony BMG was clearly motivated by revenue incentives related to digital rights to their music products, since illegal copying is a major source of revenue loss. But they had no corresponding incentives to support consumer's information security or privacy goals, nor to cooperate openly with other actors, such as platform vendors, security vendors, industry associations, consumer groups, or regulators. Likewise, incentives for consumers to act in personal or collective interests remain obscure or non-existent.

It's unlikely that current research and development efforts will be successful in the near future in making fundamental breakthroughs, especially regarding the challenge of creating widely accepted incentive instruments that get to the non-technical root causes of these problems. Therefore we call for an Initiative to mobilize and energize research and development activities across organizations, disciplines, and geographies.

In closing, we hope that this paper motivates bright and forward-thinking people to contribute their ideas, time, energy, and resources to make this Initiative a reality and great success.

10. BIOGRAPHIES

Russell Cameron Thomas – Mr. Thomas is Principal at Meritology, a consultancy that models business value and risk for information technology. He received a B.S. in Electrical Engineering and Management from Worcester Polytechnic Institute in 1980. He has held engineering and management positions at Hewlett-Packard and several start-up companies. Prior to Meritology, Mr. Thomas was a Senior Manager at BearingPoint (formerly KPMG Consulting), where he specialized in large-scale business transformation, operations improvement, and performance management. He was also Director of Research for KPMG's Valuation Services. He is a graduate of the Santa Fe Institute Summer School.

Dr. Patrick D. Amon – Dr. Amon is a Researcher at the Center for Interdisciplinary Research for Information Security, Ecole Polytechnique Federale de Lausanne (EPFL), where he is responsible for developing quantitative, data-driven risk management and valuation methodologies, and academic development of graduate students. He received a Masters and PhD in Physics from Case Western Reserve in 1997. He received an International Baccalaureate from the Ecole Internationale de Genève in 1991. Prior to EPFL, he was co-founder and Head of Research at Risk Management Group, LLC, a consultancy. He has held financial engineering research positions at ERISK, Capital Markets Co., AIG, Sailfish Systems (now part of Reuters), and Harvestons Securities. He also held research affiliations at CERN Theory Group and NYU Center for Particle Physics.

REFERENCES

1. B. Schneier, "Schneier on Security – Sony's DRM Rootkit: The Real Story", Nov.17, 2005, http://www.schneier.com/blog/archives/2005/11/sonys_drm_rootk.html .
2. R. Anderson, "Why information security is hard - an economic perspective", January 2001. http://www.cl.cam.ac.uk/~rja14/ .
3. Spafford, Eugene, "Four Grand Challenges of Trustworthy Computing", Computer Research Association, 2003. www.cra.org/Activities/grand.challenges/security/
4. B. Krebs, "Study of Sony Anti-Piracy Software Triggers Uproar", *Washington Post*, Nov. 2, 2005, http://www.washingtonpost.com/wp-dyn/content/article/2005/11/02/AR2005110202362.html
5. Cranor, Lorrie and Simson Garfinkel, *Security and Usability - Designing Secure Systems that People Can Use*, O'Reilly Media, 2005.

6. _____, "Internet Security Voter Survey", Computer Security Industry Alliance, 2005. https://www.csialliance.org/resources/pdfs/CSIA_Internet_Security_Survey_June_2005.pdf
7. _____,"Global Consumer Attitudes Toward Data Protection", Visa and Harris Interactive, Jan. 2006. www.corporate.visa.com/pd/pdf/Consumer_Global_Research_Backgrounder.pdf
8. Conference Board, "Navigating Risk—The Business Case for Security", 2006, http://www.conference-board.org/publications/describe.cfm?id=1231 .
9. B. Schneir, "How Security Companies Sucker Us With Lemons", *Wired*, April 7, 2007, http://www.wired.com/politics/security/commentary/securitymatters/2007/04/securitymatters_0419.
10. Bauckhage, Tobias, *Digital Rights Management: Economic Aspects The Basic Economic Theory of Copying*, Berlin: Springer, 2003.
11.http://www.uspto.gov/web/offices/com/speeches/houseapprop.htm
12. http://www.epic.org/privacy/terrorism/usapatriot/
13. http://en.wikipedia.org/wiki/Incentive
14. Crouhy, M., Galai, D., Mark, R., *The Essentials of Risk Management*, New York: McGraw-Hill, 2006.
15. Lam, J., *Enterprise Risk Management: From Incentives to Controls*, Hoboken, NJ: John Wiley & Sons, 2003.
16. Adams, J., *Risk: the policy implications of risk compensation and plural rationalities*, London: Routledge, 2001.
17. C.Cibrorra, "Digital Technologies and the Duality of Risk", London School of Economics, Economic & Social Research Council (ESRC), Discussion Paper #27, Oct. 2004, http://www.lse.ac.uk/collections/CARR/pdf/Disspaper27.pdf.
18. C. Starr and C. Whipple, "Risks of Risk Decisions", *Science*, Volume 208, Issue 4448, pp. 1114-1119, June 1980, http://www.sciencemag.org/cgi/content/abstract/208/4448/1114.
19. Jaquith, Andrew, *Security Metrics – Replacing Fear, Uncertainty, and Doubt*, Upper Saddle River, NJ: Addison-Wesley, 2007.
20. B. Schneier, "Information Security and Externalities", *ENISA Quarterly* (European Network and Information Security Agency), January, 2007. http://www.schneier.com/essay-150.html
21. Adam Shostack, "Avoiding Liability: An Alternate Route to More Secure Products", 4th Workshop on the Economics of Information Security (WEIS), March 6, 2005, http://infosecon.net/workshop/pdf/44.pdf .
22. Bruce Schneier, "Security and Compliance", *IEEE Security & Privacy*, July/August 2004.
23. B. C. Kim, P.-Y. Chen, T, Mukhopadhyay, "Monopoly, Software Quality and Liability", WISE 2004, http://opim.wharton.upenn.edu/wise2004/sat621.pdf .
24. C. W. Crews Jr., "Cybersecurity Finger Pointing", http://www.cei.org/pdf/4569.pdf .
25. Electronic Freedom Foundation on Digital Rights: http://www.eff.org/IP/fairuse/ .
26. Electronic Freedom Foundation on Global Online Freedom: http://www.eff.org/global/
27. C. Richardson, "Anti-trust Concerns Join Microsoft's Security Push", webpronews.com, Feb. 18, 2005, http://www.webpronews.com/news/ebusinessnews/wpn-45-20050218AntitrustConcernsJoinMicrosoftsSecurityPush.html .
28. F. A. Hayek, "The Use of Knowledge in Society", *The American Economic Review*, Vol. 35, No. 4 (Sep., 1945), pp. 519-530
29. http://en.wikipedia.org/wiki/Von_Hayek.
30. http://en.wikipedia.org/wiki/Red_queen.
31. L. Faught, "RFID for the Customer Experience – Next Wave for Retailers and Consumers", Chainlink Research, April 25, 2007, http://www.chainlinkresearch.com/research/detail.cfm?guid=B0321347-F249-AE12-9764-6CC1503CFC0D.
32. R. Anderson, "RFID and the Middleman" working paper, 2007, www.cl.cam.ac.uk/~rja14/Papers/rfid-fc07.pdf.
33. J. Schwartz "Researchers See Privacy Pitfalls in No-Swipe Credit Cards", *New York Times*, October 23, 2006, http://select.nytimes.com/gst/abstract.html?res=F5081FFE3C5B0C708EDDA90994DE404482.
34. Bitko, Gordon, "RFID in the Retail Sector – A Methodology for Analysis of Policy Proposals and their Implications for Privacy, Economic Efficiency, and Security" , PhD Dissertation, Pardee RAND Graduate School, Oct. 2006, http://www.rand.org/pubs/rgs_dissertations/2007/RAND_RGSD209.pdf.
35. _____, "Leader: RFID, NFC and consumers – What they know and need to know", Silicon.com, Oct. 22, 2004, http://networks.silicon.com/mobile/0,39024665,39125223,00.htm.
36. Hennessy, John L. , David A. Patterson, and Herbert S. Lin, (editors), *Information Technology for Counterterrorism: Immediate Actions and Future Possibilities* , Committee on the Role of Information Technology in Responding to Terrorism, National Research Council, Washington, DC: National Academies Press, 2003, http://www7.nationalacademies.org/cstb/pub_counterterrorism.html.
37. C. Landwehr, "NSF Cyber Trust Report", http://www2.gwu.edu/~usjpciip/1CyberTrust.pdf.
38. NSF Cyber Trust Program Solicitation, NSF 05-518, Last Updated: 11/07/06, http://www.nsf.gov/pubs/2005/nsf05518/nsf05518.htm .
39. Cranor, Lorrie and Simson Garfinkel, *Security and Usability - Designing Secure Systems that People Can Use*, O'Reilly Media, 2005.
40. Symposium On Usable Privacy and Security (SOUPS), http://cups.cs.cmu.edu/soups/ ; DIMACS Workshop on Usable Privacy and Security Software, http://dimacs.rutgers.edu/Workshops/Tools/
41. _____, "Information Sharing/Critical Infrastructure Protection Task Force Report", President's National Security Telecommunications Advisory Committee, May 2000.
42. Cukier, Kenneth, "Ensuring (and Insuring?) Critical Information Infrastructure Protection", Rueschlikon Conference on Information Policy, 2005. www.rueschlikon-conference.org/pressdocs/56_R_05_Report_Online.pdf
43. http://www.cert.org

44. URLs for ISAC organizations – Worldwide: http://www.wwisac.com/ , industry-specific: http://www.isaccouncil.org/about/
45. http://attrition.org/dataloss/dldos.html
46. Bugtraq mailing list: http://en.wikipedia.org/wiki/Bugtraq
47. Privacy Rights Clearinghouse: www.privacyrights.org
48. S. Pfleeger, R. Rue, J. Horwitz, A. Balakrishnan, "Investing In Cyber Security: The Path to Good Practice", Chapert 2 in *Cyber Security: Strengthening Corporate Resilience*, Cutter Consortium, 2006, https://cutter.com/cgi-bin/catalog/store.cgi?action=link&sku=RP67V&uid=6984.
49. CSI-FBI survey: http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml
50. Financial services operational risk database: http://www.algorithmics.com/solutions/opvantage/first.shtml
51. P. Ghirardato, "Coping with ignorance: unforeseen contingencies and non-additive uncertainty", Economic Theory 17, 247-276, Springer-Verlag, 2001.
52. Halpern, Joseph, *Reasoning about Uncertainty*, Cambridge, MA; MIT Press, 2003.
53. Boda, G. and Szlavik, P, "Alternative Accounting to Manage Intellectual Capital", The Electronic Journal of Knowledge Management, Vol. 5 Issue 1, p. 7-18, 2007, http://www.ejkm.com/volume-5/v5-i1/Boda_and_Szlavik.pdf
54.Amram, Martha & Nalin Kulatilaka, *Real Options: Managing Strategic Investment in an Uncertain World*, Oxfork, UK: Oxford University Press, 1998.
55. _____, "Accounting for Good: the Global Stakeholder Report 2005", Pleon, http://www.pleon.de/fileadmin/downloads/Pleon_GSR05_en.pdf
56. e.g. CMU's Center for Risk Perception and Communication: http://sds.hss.cmu.edu/risk/ .
57. Slovic, Paul, *The Perception of Risk*, London: Earthscan, 2000.
58. Morgan, M.G, Fischhoff, B., Bostrom, A., Atman, C., *Risk Communication – A mental models approach*, Cambridge, UK: Cambridge University Press, 2002.
59. M. Wilson and J. Hash, "Building an Information Technology Security Awareness and Training Program", National Institute of Standards and Technology, NIST Special Publication 800-50, Oct. 2003, http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.
60. P. Thompson and W. Dean, "Competing Conceptions of Risk", Franklin Pierce Law Center, http://www.piercelaw.edu/risk/vol7/fall/thompson.htm.
61. D. Diakoulaki,and G. Mavrotas, "Stakeholder Workshops & Multi-criteria Analysis", SusTools - Tools for Sustainability Project (Final Report on Work Package 6), National Technical University Athens, Greece, Dec. 30, 2004.
62. http://en.wikipedia.org/wiki/SimHealth and http://www.mobygames.com/game/simhealth/
63.Picard, Rosalind W., *Affective Computing*, Cambridge, MA: MIT Press, 1997.
64. http://en.wikipedia.org/wiki/Affective_computing
65. O. Stock and WP8 Members, "Report on Basic Cues and Open Research Topics in Communication and Emotions", Humaine (emotions-research.net), Oct. 11, 2004, http://emotion-research.net/deliverables/D8a.pdf
66. Ruttkay Z., Noot H., ten Hagen P., "Emotion Disc and Emotion Squares: tools to explore the facial expression face", in Computer Graphics Forum, 22 (1), 49-53, 2003.
67. ISO Information Technology – Generic coding of audio-visual objects – Part 2: visual, *ISO/IEC 14496-2 Final Draft International Standard*, 1998, Atlantic City.
68.Resnick, Paul, Zeckhauser, Richard, Friedman, Eric, and Kuwabara, Ko. Reputation Systems. *Communications of the ACM*, 43(12), December 20000, pages 45-48. http://www.si.umich.edu/~presnick/papers/cacm00/index.html . Also see: http://web.si.umich.edu/reputations/bib/bib.html
69.Verma, Dinesh C. , *Legitimate Applications of Peer-to-Peer Networks*, Hoboken, NJ: Wiley-Interscience, 2004.
70. M. Bouissou and N. Thuy, "Decision-making based on expert assessments: Use of belief networks to take into account uncertainty, bias, and weak signals", European Safety & Reliability International Conference (ESREL - Lyon, March 2002), http://perso-math.univ-mlv.fr/users/bouissou.marc/ExpertsAndBN_ESREL02.pdf .
71. Tapscott, Don and Anthony Williams, *Wikinomics: How Mass Collaboration Changes Everything*, New York: Portfolio (Penguin Group), 2006.
72. R. Ross, et. al., "Guide for the Security Certification and Accreditation of Federal Information Systems", National Institute of Standards and Technology, May 2004, http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf
73. http://www.truste.org ; http://www.scanalert.com/ ; http://www.verisign.com/
74. Edelman, Benjamin , "Adverse Selection in Online 'Trust' Certifications", Workshop on the Economics of Information Security, 2006. http://weis2006.econinfosec.org/docs/10.pdf
75. Enrico Scalas, Marco Bianchetti, Francesco Mainardi, H. Eduardo Roman and Alessandro Vivoli, "Synthetic Markets", 2003, http://www.mfn.unipmn.it/~scalas/wehia2003sm/wehia2003sm.html
76. J. Wolfers and E. Zitzewitz, "Prediction Markets". Journal of Economic Perspectives, Spring 2004.
77. L. J. Camp and C. Wolfram, "Pricing Security: Vulnerabilities as Externalities", *Economics of Information Security*, Vol. 12, 2004.
78. R. Gopal, R. Garfinkel, M. Nunez, D. Rice, "Electronic Markets for Private Information: Economic and Security Considerations", Proceedings of the 39th Hawaii International Conference on System Science 2006.
79. Böhme, Rainer, "Vulnerability Markets", 2005. http://events.ccc.de/congress/2005/fahrplan/attachments/542-Boehme2005_22C3_VulnerabilityMarkets.pdf
80.B. LeBaron, "Building the Santa Fe Artificial Stock Market", Working Paper, Brandeis University, June 2002. www.econ.iastate.edu/tesfatsi/blake.sfisum.pdf
81. Shiller, Robert J., *Macro Markets – Creating Institutions for Managing Society's Largest Economic Risks*, Oxford, UK: Oxford University Press, 1998.
82. Shiller, Robert J., *The New Financial Order: Risk in the 21st Century*, Princeton, NJ: Princeton University Press, 2003.

83. N. Karacapilidis and P. Moraïtis, "Intelligent agents for an artificial market system" , in *Proceedings of the Fifth international Conference on Autonomous Agents* (Montreal, Quebec, Canada). AGENTS '01. ACM Press, New York, NY, 592-599, 2001.
84. D. Luenberger, "Projection Pricing", Journal of Optimization Theory and Applications, Volume 109, Number 1, April 2001, pp. 1-25(25).
85. D. Luenberger, "A Correlation Pricing Formula" (working paper), Stanford University, 2002, www.stanford.edu/dept/MSandE/people/faculty/luenberger/RealOptions/CPFWeb.pdf
86. T. Cameron, G. Poe, R. Ethier, W. Shulze, "Alternative Non-market Value Elicitation Methods – Are the Underlying Preferences the Same?", Journal of Environmental Economics and Management 44, p391-425, 2002.
87. J. Kesan, R. Majuca, W. Yurcik, "Economic Case for Cyberinsurance" (working paper), University of Illinois College of Law, 2004-2.
88. L. Gordon, M. Loeb, T. Sohail, "A framework for using insurance for cyber-risk management". *Commun. ACM* 46, 3 (Mar. 2003), 81-85.
89. R. Böhme, "Cyber Insurance Revisited", presented at the 5th Workshop on Economics of Information Security (WEIS), Cambridge, MA, June 2005.
90. W. Baer, "Rewarding IT Security in the Marketplace", RAND Corporation, 2003, http://tprc.org/papers/2003/190/BaerITSecurity.pdf
91. B. C. Kim, P-Y. Chen, T. Mukhopadhyay, "An Economic Analysis Of A Software Market With Risk-Sharing Contracts", *Proceedings of the International Conference on Information Systems* (ICIS), Las Vegas, December 2005.
92. http://www.mozilla.org/security/bug-bounty.html .
93. J. Granick, "Bug Bounties Exterminate Holes", *Wired*, Apr, 12, 2006, http://www.wired.com/news/columns/0,70644-0.html
94. M. Rossi, "Insuring First-Party Cyber Risk for Fortune 1000 Companies—A Worthwhile Endeavor or Boondoggle?", International Risk Management Institute, Nov. 2002, http://www.irmi.com/Expert/Articles/2002/Rossi11.aspx .
95. L. Wood, "When all else fails, there's cyberinsurance", *Information Security* magazine, Aug. 2004, http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss446_art920,00.html .
96. T. Holmes, "Cyber Insurance: Weighing the Costs with the Risks", National Federation of Independent Business, Oct. 20, 2004, www.nfib.com/object/IO_18562.html .
97. P. Dubois, B. Jullien, T. Magnac, "Formal and Informal Risk Sharing in LDCs", Dec. 2006, submitted to *Econometrica*, http://www.toulouse.inra.fr/centre/esr/CV/dubois/djm.pdf .
98. E. Briys and F. Célimène, "Globalisation and Risk Sharing: Debunking Some Common Pitfalls", presented at Colloque International sur les Impacts Economiques et Politiques de la Mondialisation, Port-au-Prince , Haïti, September 2004, http://cyberlibris.typepad.com/blog/files/Haiti2.doc .
99. Y. Bramoullé, R. Kranton, "Risk Sharing Networks", Centre Interuniversitaire sur le Risque, Les Politiques Économiques et l'Emploi, Working Paper 05-26, Sep. 2005.
100. V. G. Narayanan and A. Raman, "Aligning Incentives in Supply Chains", *Harvard Business Review*, Nov. 2004, p 94-102.
101. R. Gulati, "Increasing the Odds: Creating and Managing Intelligent Alliances" (presentation), Kellogg Graduate School of Management, Northwestern University, 2001.
102. J. Cruz, A. Nagurney, T. Wakolbinger, "Financial Engineering of the Integration of Global Supply Chain Networks and Social Networks with Risk Management", *Naval Research Logistics* 53 (2006), p 674-696.
103. T. Hogg and B. Huberman, "Taking risk away from risk taking: decision insurance in organizations", HP Labs working paper, April 13, 2006, www.hpl.hp.com/research/idl/papers/insurance/insurance.pdf.
104. H. Kunreuther and G. Heal, "Interdependent Security", *Journal of Risk and Uncertainty* 26, p 231-249, 2003.
105. D. Krueger and H. Uhlig, "Competitive Risk Sharing Contracts with One-sided Commitment", CFS Working Paper Series 2005/07, Center for Financial Studies, 2005.
106. F. Wallenberg, "Aligning Incentives in Copyright – A Soft Approach to Fair Use", UC Berkeley working paper, May 9, 2002. www.ischool.berkeley.edu/~fredrik/research/papers/AligningIncentives.pdf
107. J. Kelsey and B. Schneier, "Electronic Commerce and the Street Performer Protocol", published in *The Third USENIX Workshop on Electronic Commerce Proceedings*, USENIX Press, November 1998.
108. http://en.wikipedia.org/wiki/Street_Performer_Protocol
109. C. Rasch, "The Wall Street Performer Protocol: Using Software Completion Bonds to Fund Open Source Software Development", *First Monday* 6-6, 2001. http://www.firstmonday.org/issues/issue6_6/rasch/index.html
110. P. Dorrell, "Published Digital Information is a Public Good: The Case for Voted Compensation", Mar. 2, 2005. http://www.1729.com/ip/PublicGood.html
111. P. Dorrell, "Looking for a Win/Win Solution to the War Between 'Premium Content' and Digital Freedom", Dec. 26, 2006, http://www.1729.com/blog/LookingForAWinWin.html .
112. V. Bergelson, "It's Personal but Is It Mine? Toward Property Rights in Personal Information", Rutgers Law School (Rutgers), Faculty Papers, Paper 33, 2003, http://law.bepress.com/rutgersnewarklwps/fp/art33 .
113. S. Besen, S. Nataraj Kirby "Compensating Creators of Intellectual Property", RAND Corporation, 1989. http://www.rand.org/pubs/reports/R3751/
114. K. van Wyk, "Updating our Thinking on Software Updates" eSecurityPlanet.com, May 3, 2005, http://www.esecurityplanet.com/views/article.php/3502176 .
115.S. Garfinkel, "The Evil Side of Automatic Software Updates", CSOonline.com, Oct. 09, 2006, http://www.csoonline.com/read/100106/col_machine_pf.html .
116. Andy, "DRM Hell", BentUser.com, Dec. 31, 2005, http://www.bentuser.com/article.aspx?ID=330
117. K. Biglione, "Zune's Big Innovation: Viral DRM", Medialoper.com, Sep. 15, 2006, http://www.medialoper.com/hot-topics/music/zunes-big-innovation-viral-drm/ .

118. E. Felten, "DRM Wars: The Next Generation", *Freedom to Tinker* (blog), August 9, 2006, http://www.freedom-to-tinker.com/?p=1051.
119. P. Gutmann, "A Cost Analysis of Windows Vista Content Protection", updated: Jan 23, 2007, http://www.cs.auckland.ac.nz/~pgut001/pubs/vista_cost.html .
120. R. Walsh, "Valuing Security Products and Patches" (presentation), CITI, University of Michigan, June 4, 2004.
121. The Economist, "Putting it all together – Security spending is a matter of balancing risks and benefits" , Oct. 24, 2002.
122. J. Downs, M. Holbrook, and L. Faith Cranor, "Decision Strategies and Susceptibility to Phishing", presented at *Symposium on Usable Privacy and Security*, Pittsburg PA, July 12-14, 2006, http://cups.cs.cmu.edu/soups/2006/proceedings/p79_downs.pdf.
123. J. Proulx "Crying wolf? – When and how to alert the public of possible terrorist attacks", University of Minnesota News, August 13, 2004, http://www1.umn.edu/umnnews/Feature_Stories/Crying_wolf_when_and_how_to_alert_the_public_of_possible_terror_attacks.html .
124. B. Kam, "Managing Outsourcing Risks in the Global Supply Chain: An Exploration of Approaches, presented at *International Trade and Logistics, Corporate Strategies and the Global Economy* (International Conference), University of Le Havre, Sept. 28-29, 2005.
125. K.-M. Bryson and W. Sullivan, "Designing effective incentive-oriented contracts for application service provider hosting of ERP systems", *Business Process Management Journa*l, Vol. 9 No. 6, 2003, p. 705-721, http://www.ituniv.se/program/sem_research/Publications/2003/Sul03/BPMJ9-6Final.pdf.
126. J. Goo and K. Nam, "Contract as a Source of Trust – Commitment in Successful IT Outsourcing Relationships: An Empirical Study", *Proceedings of the 40th Hawaii International Conference on System Sciences*, 2007, www.hicss.hawaii.edu/hicss_40/decisionbp/09_11_01.pdf.
127. _____, "Kalculator: BITS Key Risk Measurement Tool for Information Security Operational Risks", BITS (Financial Services Roundtable, 2004, http://www.bitsinfo.org/downloads/Publications%20Page/BITS%20Kalculator/bitskalcnarrative.pdf.
128. D. Simons, "ID Theft Insurance Isn't Insurance", *Forbes*, May 29, 2003, http://www.forbes.com/2003/05/29/cx_ds_0529simons.html.
129 iDefense: http://labs.idefense.com/vcp/.
130. S. Shankland, "Sun launches open-source digital rights plan", CNET News.com, August 21, 2005, http://news.com.com/Sun+launches+open-source+digital+rights+plan/2100-1025_3-5840492.html.
131. http://www.openmediacommons.org/.
132. "Patchy DRM": http://www.pachydrm.org/
133. http://odrl.net/.
134. _____, "MEF mDRM White Paper: An Introduction to Mobile Digital Rights Management (mDRM)", prepared by Booz, Allen, Hamilton for Mobile Entertainment Forum (MEF), Nov. 2005, http://www.amplefuture.com/assets/pdfs/MEF_DRM_20Whitepaper_Nov_05.pdf.
135. E. Van Buskirk, "Reasons to Love Open-Source DRM", *Wired Magazine*, April 3, 2006, http://www.wired.com/entertainment/music/commentary/listeningpost/2006/04/70548?currentPage=1.
136. L. Lessing, "openDRM", Mar. 23, 2006, http://www.lessig.org/blog/archives/003353.shtml .
137. M. Hines, "Digital content spurs micropayments resurgence", CNET News.com, September 7, 2004, http://news.zdnet.com/2100-3513_22-5347513.html.
138.T. Mornini and L. Walley, "Bringing Pay-per-view to the Masses", FaceBridge, 2006, http://facebridge.com/facebridge_support_data.pdf.
139. _____, "Software Providers Should Accept Responsibility for Their Role in Supporting US Financial Institutions and Critical Infrastructure", BITS/Finanical Services Roundtable press release, April 27, 2004, www.bitsinfo.org/downloads/Misc/bitssoftsecuritypolicyapr04.pdf.
140. R. Anderson, "Why information security is hard - an economic perspective", January 2001. http://www.cl.cam.ac.uk/~rja14/ .
141. K.-M. Osei-Bryson and O. Ngwenyama, "Structuring IS Outsourcing Contracts for Mutual Gain: An Approach to Analyzing Performance Incentive Schemes", *Journal of the Association for Information Systems*, Vol. 1, November 2000.
142. K.-M. Osei-Bryson and O. Ngwenyama, "Managing risks in information systems outsourcing : An approach to analyzing outsourcing risks and structuring incentive contracts", *European Journal of Operational Research*, Vol. 174, No 1, 2006, pp. 245-264.
143. J. Goo, D. Kim, and B. Cho, "Structure of Service Level Agreements (SLA) in IT Outsourcing: The Construct and it's Measurement", in *Proceedings of the 12th Americas Conference on Information Systems* (AMCIS), Acapulco, Mexico, 2006.
144. Dembo, Ron, Aziz, A., Rosen, D., and Zerbs, M., *Mark-to-Future – A framework for measuring risk and reward*, Toronto: Algorithmics Publications, May 2001, http://www.algorithmics.com/research/MarktoFuture/toc.shtml .
145. "Symantec Launches Internet Threat Meter for Yahoo! Widget", June 14, 2006, http://www.geekzone.co.nz/content.asp?contentid=6360
146. A. Acquisti, J. Grossklags, "Uncertainty, Ambiguity, and Privacy", 4th Annual Workshop on the Economics of Information Security (WEIS 2005). http://infosecon.net/workshop/pdf/64.pdf
147. P. Syverson, "The Paradoxical Value of Privacy", March 14, 2003, In 2nd Annual Workshop on Economics and Information Security - WEIS '03, 2003.chacs.nrl.navy.mil/publications/CHACS/2003/2003syverson-privcost.pdf
148. J. Ryan, "The Use, Misuse, and Abuse of Statistics in Information Security Research", Presented to American Society of Engineering Management National Conference (ASEM 2003, St. Louis, MO), http://www.seas.gwu.edu/~jjchryan/asem03.pdf.
149. B. Mandelbrot and N. Taleb, "A Focus on the Exceptions that Prove the Rule", *Financial Times*, March 23 2006, http://www.ft.com/cms/s/5372968a-ba82-11da-980d-

0000779e2340,dwp_uuid=77a9a0e8-b442-11da-bd61-0000779e2340.html.
150. Crosby, Phillip, *Quality Is Free: The Art of Making Quality Certain*, New York: McGraw-Hill, 1979.
151. http://www.asq.org/learn-about-quality/cost-of-quality/overview/overview.html
152. http://en.wikipedia.org/wiki/RAROC
153. http://www.riskglossary.com/link/economic_capital.htm.
154. http://en.wikipedia.org/wiki/Economic_value_added
155. R. Thomas, "Total Cost of (In)security", presented at Mini-Metricon, February 2007, http://meritology.com.
156. R. Thorton, "Software Quality is not Software Security", http://extra.fortifysoftware.com/blog/2006/08/software_quality_is_not_softwa.html .
157. J. Kelsey and B. Schnier, "The Street Performer Protocol", In The Third USENIX Workshop on Electronic Commerce Proceedings. USENIX Press, November 1998.
158. http://www.geocities.com/socialpbonds/
159. C Rasch, "Wall Street Performer Protocol: Using Software Completion Bonds to Fund Open Source Software Development", First Monday, volume 6, number 6, June 2001, http://www.firstmonday.org/issues/issue6_6/rasch/index.html
160. http://en.wikipedia.org/wiki/Experimental_economics
161. http://en.wikipedia.org/wiki/Scenario_analysis
162 Shirreff, David, *Dealing with Financial Risk*, New York: Bloomberg Press, 2004.
163. Joseph Y. Halpern, *Reasoning About Uncertainty*, Cambridge, MA: MIT Press, 2005.
164. http://en.wikipedia.org/wiki/Prediction_market
165. http://secondlife.com
166. Rymaszewski, Michael, et. al., *Second Life – the official guide*, Hoboken, NJ: John Wiley & Sons, 2006.
167. L. Zimmer, "Intellectual Property Rights in Virtual Places", *Business Communicators of Second Life* (blog), March 4, 2006, http://freshtakes.typepad.com/sl_communicators/2007/03/intellectual_pr.html .
168. J. Granick, "Second Life Will Save Copyright", *Wired Magazine*, Nov. 20, 2006, http://www.wired.com/gaming/virtualworlds/commentary/circuitcourt/2006/11/72143.
169. C. Samiam, "Linden Lab Supports Invasion of Your Privacy?", *Second Life Herald*, March 25, 2005, www.secondlifeherald.com/slh/2005/03/linden_lab_supp.html.
170. _____, "Second Life Security Bulletin", Linden Labs press release, September 8, 2006, http://secondlife.com/corporate/bulletin.php.
171. B. Golze, "MMORPG currency exchange defrauded for $3,000", *Gamespot*, June 23, 2004, http://www.gamespot.com/news/6101196.html.
172. C. Ondrejka, "Escaping the Gilded Cage – User-created Content and Building the Metaverse", in *The State of Play – Law, Games, and Virtual Worlds* (Jack Balkin and Beth Simone Noveck, eds.), New York: New York University Press, 2006, p. 174,
173.http://www.simteach.com/wiki/index.php?title=Institutions_and_Organizations_in_SL#UNIVERSITIES.2C_COLLEGES_.26_SCHOOLS
174. R. Thomas, "The Cyber Trust R&D Landscape", (forthcoming 2007), http://meritology.com,
175. Wenger, Etienne, Richard McDermott, William M. Snyder, *Communities of Practice*, Cambridge, MA: Harvard Business School Press, 2002.
176. G. O'Connor and A.Ayers, "Building A Radical Innovation Competency", *Research-Technology Management*, Volume 48, Number 1, January-February 2005, pp. 23-31(9), http://www.iriinc.org/Template.cfm?Section=Home&CONTENTID=3165&TEMPLATE=/ContentManagement/ContentDisplay.cfm .
177. Leifer, Richard, Christopher M. McDermott, Gina Colarelli O'Connor, Lois S. Peters, Mark P. Rice, Robert W. Veryzer, Mark Rice, *Radical Innovation: How Mature Companies Can Outsmart Upstarts*, Cambridge, MA: Harvard Business School Press, 2000.
178. Waldrop, M. Mitchell, *Complexity: The Emerging Science at the Edge of Order and Chaos*, New York: Simon & Schuster 1992.
179. _____, "Nurturing and Executing Innovation", Thought Leadership Roundtable on Digital Strategies, Tuck School of Business, 2006, http://mba.tuck.dartmouth.edu/digital/Programs/CorporateEvents/Innovation/Overview.pdf.
180. B. du Toit, "Risk, Theory, Reflection: Limitations of the stochastic model of uncertainty in financial risk analysis", June 2004, www.riskworx.com/insights/theory/theory.pdf.
181. T. Nilsen and T. Aven, "Models and model uncertainty in the context of risk analysis", *Reliability Engineering and System Safety*, Volume 79, Number 3, 1 March 2003, pp. 309-317(9), http://risikoforsk.no/Publikasjoner/ModUsRESS2.pdf.
182. Wenger, Etienne, Richard McDermott, William M. Snyder, *Communities of Practice*, Cambridge, MA: Harvard Business School Press, 2002.
183. Von Hippel, Eric, *Democratizing Innovation*, Cambridge, MA: The MIT Press, 2006.
184. V. Vlachos, S. Androutsellis-Theotokis, D. Spinellis, "Security Applications of Peer-to-Peer Networks", *Computer Networks*, 45:195-205, 2004. http://www.spinellis.gr/pubs/jrnl/2004-CompSec-p2pav/html/VAS04.pdf
185. B. C. Stahl, "Privacy and Security as Ideology", *IEEE Technology and Society* (26:1), special issue on "Usable Security and Privacy", edited by L. Jean Camp, 35 - 45 2007. http://www.cse.dmu.ac.uk/~bstahl/publications/2006_Privacy_Security_Ideology_LSPI.pdf
186. _____, "Federal Plan for Cyber Security and Information Assurance R&D 2006", Interagency Working Group on Cyber Security and Information Assurance, April 2006. www.nitrd.gov/pubs/csia/csia_federal_plan.pdf
187. _____, "Cyber Security: A Crisis of Prioritization (Report to the President)", President's Information Technology Advisory Committee, Feb. 2005. www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf
188. Cukier, Kenneth, "Ensuring (and Insuring?) Critical Information Infrastructure Protection", Rueschlikon Conference on Information Policy, 2005. www.rueschlikon-conference.org/pressdocs/56_R_05_Report_Online.pdf

189. Committee on Improving Cybersecurity Research in the United States, Computer Science and Telecommunications Board (CSTB), National Academies, http://www7.nationalacademies.org/cstb/project_cybersecurity_sow.html.
190. Joint Venture/Silicon Valley "Smart Health" initiative, http://www.jointventure.org/programs-initiatives/smarthealth/smarthealthmain.html.
191. B. Andersen, R. Kozul-Wright and Z. Kozul-Wright, "Rents, Rights N' Rhythm - Conflict and Cooperation in the Music Industry", Workshop on Network Theme 2 (Globalisation, Convergence and Divergence), AHRC Research Network, Birkbeck School of Law, University of London, 2004 www.copyright.bbk.ac.uk/contents/publications/workshops/theme2/banderson.pdf
192. Gerd Leonhard, 'The Future of TV", March 21, 2007. http://www.gerdpresents.com/files/itv_march_21_2007_london_web.pdf
193. http://en.wikipedia.org/wiki/Software_as_a_service
194. J. Hagel III and J.S. Brown, "Your Next IT Strategy", *Harvard Business Review*, October 2001, pp. 105-113
195. M. Mailani and J. S. Brown, "Some Security Considerations for Service Grids", (white paper), April 2002, http://www.johnhagel.com/paper_securitygrid.pdf.
196. _____, "Securing the cloud", *The Economist*, Oct 24, 2002, www.economist.com/surveys/displaystory.cfm?story_id=1389589.
197. "P2P File Sharing Applications", http://www.sans.org/top20/#c3.
198. M.P.C. Weijnen, I. Bouwmans, L.J. de Vries, "Coping with Critical Infrastructures – steering multi-actor decision making", Presentation at the 2005 General Conference of The International Risk Governance Council: Implementing a Global Approach to Risk Governance, 20th Sep. 2005. At: Beijing, China.
199. W. Wong, "Protecting Soft IP", *Electronic Design Online*, April 14, 2005, http://www.elecdesign.com/Articles/Index.cfm?AD=1&ArticleID=10084.
200. W. Adi,, R. Ernst, B. Soudan, A. Hanoun,"VLSI design exchange with intellectual property protection in FPGA environment using both secret and public-key cryptography",. IEEE Computer Society Annual Symposium on Emerging VLSI Technologies and Architectures, 2006. March 2006,
201. Sheffi, Yossi, *The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage*, Cambridge, MA: MIT Press, 2005.
202. Brindley, Clare (ed.), *Supply Chain Risk*, Burlington VT: Ashgate Publishing Ltd., 2004.
203. Rao, Ramesh R., Jon Eisenberg, and Ted Schmitt (editors), *Improving Disaster Management: The Role of IT in Mitigation, Preparedness, Response, and Recovery*, Committee on Using Information Technology to Enhance Disaster Management, National Research Council, Washington, DC: National Academies Press, 2007, http://books.nap.edu/catalog.php?record_id=11824.
204. B. Snow, "What we need is assurance", Annual Computer Security Applications Conference, 2005, www.acsac.org/2005/papers/Snow.pdf
205. D. Chmielewski, "Yahoo sued over data on Chinese dissidents", Los Angeles Times, April 19, 2007, http://www.latimes.com/technology/la-fi-yahoo19apr19,1,5219909.story?coll=la-headlines-technology.
206. K. Poulsen, "Secrecy Power Sinks Patent Case",*Wired*, Sept. 20, 2005, http://www.wired.com/science/discoveries/news/2005/09/68894.
207. J. Risen And E. Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts", *New York Times*, Dec. 15, 2005, http://www.nytimes.com/2005/12/16/politics/16program.html?ex=1292389200&en=e32070e08c623ac1&ei=5089
208. http://weis2006.econinfosec.org/