

Incentive-based Cyber Trust – Call to Action

Summary

“Cyber trust” is the confluence of information security, privacy, digital rights, and intellectual property (IP) protection, from social and economic perspectives. A prime example of this confluence is the recent case of Sony BMG Music Entertainment who, in 2005, distributed a copy-protection scheme with their music CDs that secretly installed a root kit* on computers that played the CDs. This case and others show that many problems in cyber trust exist at least partially because the people and institutions involved are not properly motivated to solve them, or that one party’s “solution” increases risks or costs for others. In essence, the incentives for stakeholders are often perverse, misaligned, or missing. 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 computer 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.

The incentive-based approach applies free market economics to situations that have previously only been managed through command-and-control, with potential for corresponding advantages and benefits – more efficiency, greater adaptability, more innovation, and greater social welfare. The NSF Cyber Trust vision is for a world in which networked computer and communication 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. The incentive-based approach adds these elements to the vision:

- Managed and used by people who are well informed about information risk and have the ability to manage risk/reward tradeoffs;

* A “root kit” can allow someone else to gain and maintain access to your computer system without your knowledge.

- 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;
- 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.

Incentive-based cyber trust will require research and innovation in the following areas:

- **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.
- **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 incentive-based approach is complementary to, but different from other approaches to cyber trust. Other approaches include the *technological approach* (i.e. “We can target and subdue the cyber threats with technology and tools.”), the *mandates approach* (i.e. “Do this...”), the *penalty-based approach* (i.e. “...or else!”), *political approach* (i.e. “Change the power structure, and good things will follow.”). In contrast, the *incentive-based approach* essentially 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.” 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.

To succeed, the incentive-based approach requires that we develop 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. It is based on modern risk management methods and experience. 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. Therefore, the incentive-based approach requires sophisticated and robust models for risk in the face of sparse information and many uncertainties. The goal of risk management is to balance the expected value of losses with the costs for mitigating those losses. This does not necessarily imply purely quantitative models or monetary valuations. The sociological aspect of risk management incorporates ideas such as qualitative values, risk tolerance/aversion, bias, risk perception, and motivational dynamics

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. But this is about to change. Many innovative solutions could be created if the research goals mentioned above are achieved. Here are brief descriptions of several practical applications:

1. **Risk-sharing instrument for information and computing technology (ICT) products and services** – these risk-sharing instruments would be some form of forward contract on predefined cash flows from both ICT vendors and customers, approximating their cyber trust self-insurance costs. This would provide compelling incentives for the ICT vendors and customers to share cyber trust information and work more cooperatively to implement cost-effective cyber trust solutions.
2. **Real-time cyber risk dashboard for end users and consumers** – 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. 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).
3. **Enterprise Total Cost of (In)Security** – To guide investments and decision-making, new managerial accounting methods and decision support tools are needed to measure the Total Cost of Security (or Insecurity). It would also

serve as the basis for risk sharing and other incentive instruments, and also allow meaningful public disclosure of cyber trust risks in stakeholder reports.

4. **Incentive funds for vulnerability research and resolution** – stakeholder contribution schemes and/or completion bonds. People could place donations to support vulnerability research in escrow, to be released to a security researcher or software vendor in the event that the promised vulnerability discovery and resolution is put in the public domain. The process would be managed and assured by trusted third parties. The benefit of this approach is that it provides funding up front for speculative but socially valuable activities (i.e. vulnerability research) and it makes the economic incentives more visible.
5. **Simulation games and simulated markets for cyber risk valuation** – these and other tools from experimental economics could be used to generate forward-looking cyber trust valuation data that are currently missing. Plausible simulation models would be built and then the simulations would be run across many scenarios and parameter values in Monte Carlo fashion. While not a forecast or prediction of future events, these methods might yield robust, forward-looking risk metrics and valuations in the fast-changing cyber trust environment.

Early adopters of the first incentive-based cyber trust solutions will probably be in industries/sectors where cyber trust is most critical – e.g. financial services, health care services, software and information services, critical infrastructure, national security, and electronics supply chain.

To achieve the research goals, we believe it's necessary to launch an organized Initiative as a virtual organization. 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.