ECONOMIC ANALYSIS OF THE U.S CYBER SECURITY INFRASTRUCTURE

Introduction

This interview is in support of a study being funded by the National Institute of Standards and Technology (NIST). NIST has contracted with RTI International to conduct an economic analysis of the cyber security technical infrastructure needs of U.S. industries. RTI's primary task is to estimate both inefficient spending (proactive and reactive spending) and the costs (spending and losses) of insufficient cyber security as a result of an inadequate cyber security infrastructure. This information will help NIST and the federal government more broadly to make the most efficient investments aimed at improving cyber security based on the net economic impact to the U.S. economy. Your participation in this data collection exercise is completely voluntary.[1]

Non-Disclosure Policy

RTI has a well-established practice of dealing with confidential information as part of numerous projects. Any information we obtain through these interviews will be used solely in aggregate with other information garnered from other interviews. In no instance will specific individuals or organizations be identified by name in any reports or as part of information which is released publicly or to NIST based on our discussions.

Discussion Guide

The following questions form a discussion guide that we would like to use to frame our conversation. We anticipate having a conversation with you about cyber security issues in your industry. Although we will not ask questions verbatim, we have prepared the following questions to provide you with a deeper sense of the topics we would like to explore during our discussion.

Security Threats

- Do you consider IT security to be a significant concern?
- What specific IT security vulnerabilities are you most concerned with?
- To what IT security problems do you dedicate the greatest amount of resources?

[1] **NOTE:** This questionnaire contains collection of information requirements subject to the Paperwork Reduction Act (PRA). Notwithstanding any other provisions of the law, no person is required to respond to, nor shall any person be subject to penalty for failure to comply with, a collection of information subject to the requirements of the PRA, unless that collection of information displays a currently valid OMB Control Number. The estimated response time for this questionnaire is 30 minutes. The response time includes the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this estimate or any other aspects of this collection of information, including suggestions for reducing the length of this questionnaire, to the National Institute of Standards and Technology, Attn., Greg Tassey, gregory.tassey@nist.gov, Mail Stop 1060 100 Bureau Drive Gaithersburg, MD 20899, 301-975-2663. The OMB Control No. is 0693-0033, which expires on 10/31/2012.

- What are the impacts of an IT security incident to your company? In what way might you experience monetary loss as a result of IT incidents (i.e. downtime, theft of private information, etc.)?

- What IT security concerns do you currently see as you look into the future at technologies your company is likely to use—cloud computing / virtualization, increased use of mobile devices, increased use of social media, etc.? Why are you concerned—i.e., what IT security infrastructure/solutions are missing as you look forward?

Security Strategies and Technologies

- Do you feel that the technologies you use to combat IT security threats have provided a significant return on investment (ROI)? How could these technologies be improved to increase the ROI?

- What are the barriers to adopting IT security technologies in your company?

- Do you see any current IT security threats for which there is not a good solution or no solution at all?

- Do you face any mandates which control your IT security strategy (e.g., from clients or regulation)?

- Are your IT security solutions developed internally or purchased from outside vendors? If the latter, which ones? How did/do you decide where to purchase your IT security technologies?

- Do you use any best practices or recommended guidelines from the government or other nonprofit organizations (e.g., industry associations)? If so, which ones?

- Do you track the number of IT security events that occur at your company and/or the resources used to resolve them? Do you track downtime and other costs as a result of IT security events?

- Would you describe your IT security strategy as largely proactive or reactive? What percentage of time do you spend responding to threats reactively—including large breaches, DDoS attacks, as well as viruses, worms, and malware on individual machines?

- How often do you review IT security strategies and spending and make any necessary changes? Discuss the process.

Security Spending

- As a percentage of your company's IT budget, how much did you spend on IT security last year—hardware, software, and labor combined?
- Do you believe that your organization is currently spending an appropriate amount of resources on IT security?
- On what areas do you think your spending is least effective (i.e., you're spending too much for the IT security improvement you gain)? Why is this spending not as effective as you would like?
- If you had a 25% increase in your IT security budget, what would you spend it on? Why don't you spend as much money on this area today?
- How much did you spend on IT security infrastructure R&D last year—e.g., developing standards to work with your customers, committing staff to work at industry consortia, etc.?
- Do you know of other government agencies, associations, or companies conducting similar R&D activities?
- Do you participate in any industry associations or consortia? Do they develop standards or best practice documents?

Manufacturing-Specific Questions

- What aspects of the manufacturing process are most vulnerable to IT security threats?
- How do IT security problems in one step of the supply chain affect other parts of the process?
- How has Sarbanes-Oxley affected your IT security level/monitoring?
- How do your company's downstream customers' levels of IT security affect your IT security decisions?

Healthcare-Specific Questions

- How are patients' privacy concerns protected through IT security?
- How do patients' needs conflict with IT security decisions?
- How does HIPAA affect your IT security purchases/procedures/policies?
- Please describe your opinion of HIPAA and other regulations to which you adhere. Do they adequately prepare you for the level of IT security you need? Do you think they are helping?

- How have federal and state breach disclosure laws affected your spending on IT security?

Utility- Specific Questions

- How do you respond to NERC's recommendations related to IT security?
- Do state utilities commissions regulate your IT security activities?
- How do you respond to Congressional/GAO/DHS recommendations related to IT security?
- Do you estimate the potential impacts of an IT security compromise on your electricity service offerings? If so, how does this affect the level of security you maintain?

Finance-Specific Questions

- How does Gramm-Leach-Bliley affect your IT security purchases/procedures/policies?
- Please describe your opinion of Gramm-Leach-Bliley and other regulations to which you adhere. Do they adequately prepare you for the level of IT security you need? Do you think they are helping?
- How have federal and state breach disclosure laws affected your spending on IT security?

Telecommunications-Specific Questions

- How does regulation or guidance from the Federal Communications Commission (FCC) affect your IT security currently—both your internal company security and the security you provide to customers?

Retail Questions

- How does the Payment Card Industry Data Security Standard (PCI DSS) affect your security policies?
- What precautions are taken to protect cardholder data?
- How have federal and state breach disclosure laws affected your spending on IT security?