October 2012

Cyber Security Test Bed

Project Leads

Brent Rowe, RTI International

Katrina Ladd, RTI International

Charlotte Scheper, RTI International

S. Cornelia Kaydos-Daniels, RTI International

Kemal Piskin, Applied Research Associates

Joan Myers, Applied Research Associates

Introduction

The inadequacy of U.S. small and medium businesses' cyber security poses great risk to these businesses and to all U.S. organizations and individuals.[1] To test strategies for improving the level of cyber security maintained by small and medium businesses in the United States, RTI International and Applied Research Associates (ARA) launched the Cyber Test Bed to establish a framework for identifying and testing best practices in cyber security specifically targeted at small and mid-size businesses. A simple, scalable methodology for reducing cyber security risks was developed and tailored to each company based on threat data and information collected on each company's cyber security infrastructure (hardware, software, policies, and procedures).

[1] According to a study by Javelin Strategy and Research (2011), the impact of data and identify theft aimed at small businesses was approximately $8 billion in 2010, with $5.43 billion in losses being borne by small and medium businesses. Losses and costs resulting from the inadequate cyber security of these businesses, which represent over 99% of U.S. companies (Small Business Administation, 2011), have an impact on not only these companies but also on their customers, clients and partners which comprise all U.S. individuals and organizations.

More than 65 companies were considered and evaluated for participation. Of those companies, 13 were selected for recruitment into the project. The companies included a law firm, an information technology services firm, a commercial real estate firm, a venture capital firm, a nonprofit education research organization, a semiconductor materials company, a nonprofit telecommunications organization, and a prefabrication construction company. The companies ranged in size from 1 to 160 employees and company revenues ranged from $100,000 per year up to $15.5 million per year.

The Cyber Test Bed team recommended tools, models, training, mitigation strategies, and policy frameworks for each company. Although each company was provided the same categories of information, the specific information and training that were provided and the solutions that were tested were tailored to each company. Nine small and mid-size businesses were recruited to participate in the Cyber Test Bed, and over a 1-year period, they were each exposed to the core Test Bed components. During that period, companies invested an average of almost 120 hours participating in or as a result of the Test Bed experience.

To evaluate the effectiveness of the Test Bed in influencing changes in cyber security perceptions and behavior, pre- and post-Test Bed interviews were conducted to ascertain a baseline and evaluate changes against that baseline that could be attributed to participation in the Test Bed. Each of the pre- and post-interviews was conducted with at least two employees at each of the nine companies. During the pre-Test Bed interviews, the aim was to ascertain the status of each company's knowledge, perceptions, and behaviors related to cyber security. After each company participated, a second round of interviews was conducted to determine how companies' knowledge, perceptions, and behaviors related to cyber security changed, and how they viewed the Test Bed experience.

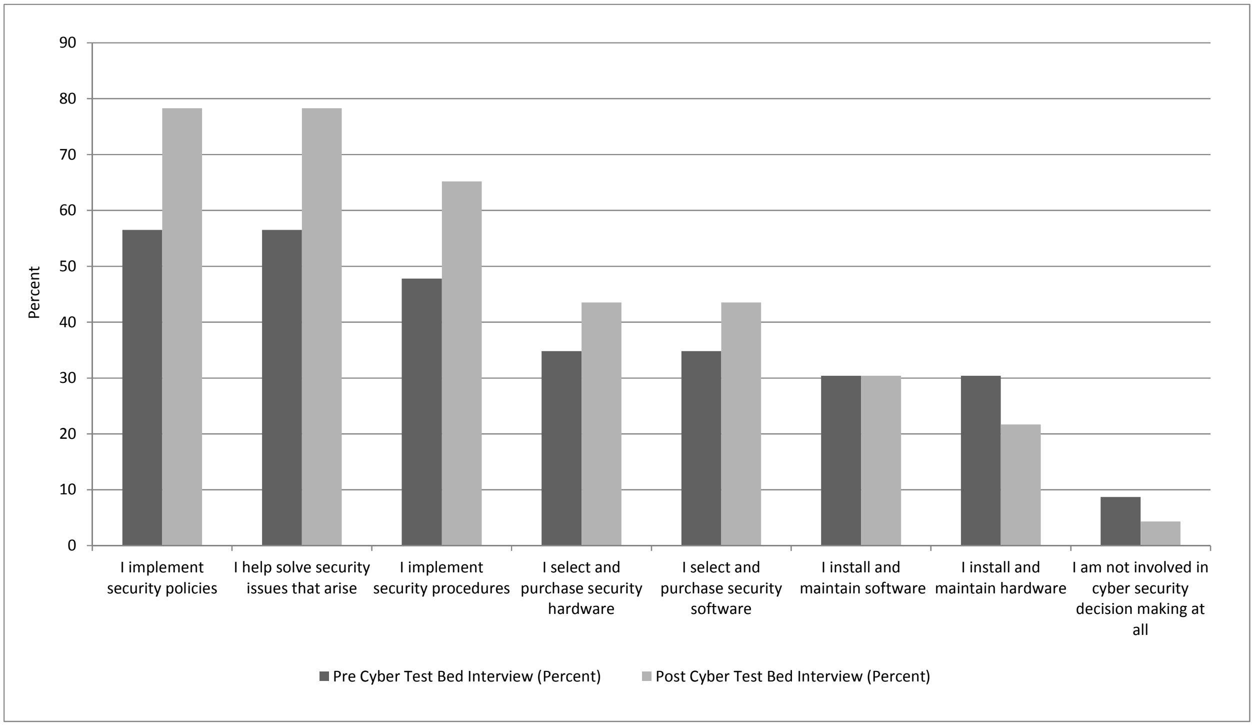
Twenty-three individuals participated in interviews both before and after participating in the Cyber Test Bed. Of those, 9 individuals characterized themselves as cyber security decision makers in their organizations, while 14 did not. This was a critical distinction when analyzing the results of the interview data collected.

The data we collected and the results of the subsequent analyses provide a useful case study of how a set of cyber security educational tools can have an impact on a set of small businesses. The results suggest an increase in time and money spent on cyber security, an increase in the perceived level of risk from cyber security, and an increase in the perceived level of knowledge of cyber security threats and solutions by participants.

Cyber Security Behaviors

The results of the interviews suggest that participants in the Cyber Test Bed generally increased the percent of their time spent on cyber security after the Test Bed, from 1.78% to 4.89%, respectively. After participation in the Cyber Test Bed, interview results also suggest an increase in the number of participants who had implemented cyber security policies and procedures and helped solve security issues that arose (Figure 1 shows this change in several areas of cyber security activities).

Figure 1. Involvement in Cyber Security Decision Making

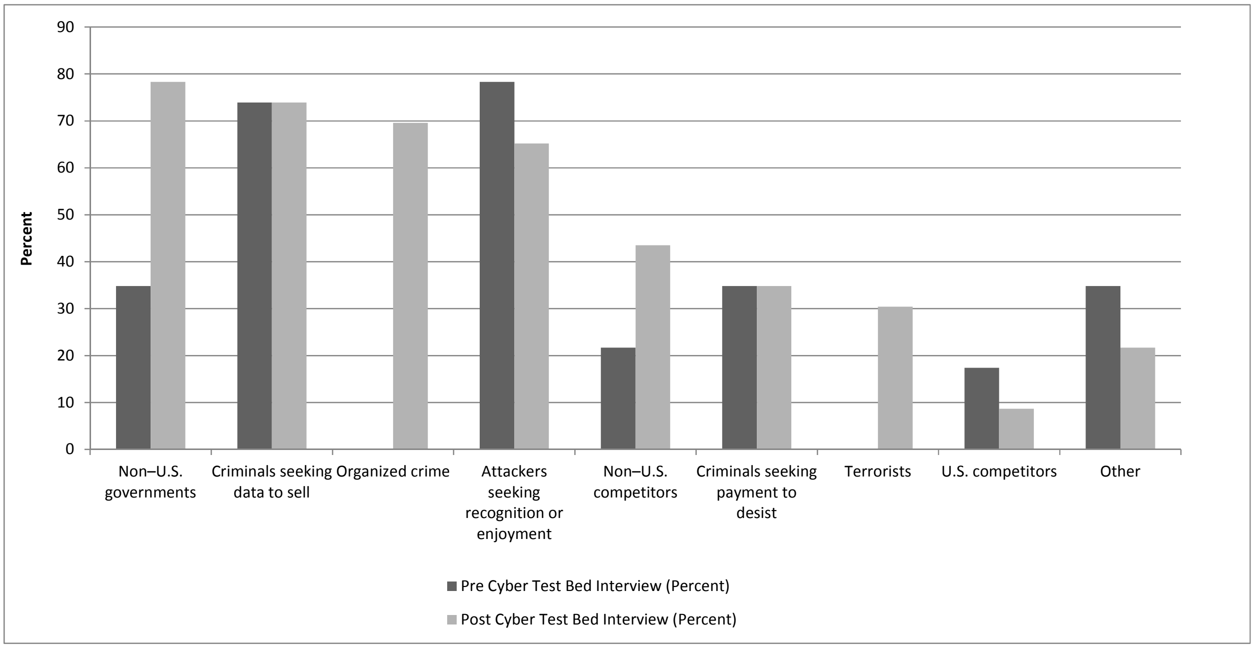


Cyber Security Perceptions

Cyber security perceptions also appear to have changed as a result of participation in the Cyber Test Bed. After the Cyber Test Bed, the average level of concern about cyber security expressed by interview participants decreased by approximately 18%. After the Test Bed, fewer individuals felt that their companies send the appropriate amount of money on cyber security (only 26.1 % as compared to 47.8% prior to the Cyber Test Bed); companies indicated a need to increase their spending.

In terms of the sources of potential attacks, companies changed their perceptions significantly after the Cyber Test Bed experience (see Figure 2). Before the Test Bed, many companies believed that the primary sources of cyber attacks were attackers seeking recognition or enjoyment, whereas after the Test Bed, companies' concern about non-U.S. governments increased and companies became concerned about organized crime and terrorists, which had not been recognized as a potential threat prior to the Test Bed. Criminals seeking to steal company data were a significant concern both before and after the Test Bed.

Figure 2. Potential Sources of Cyber Attacks



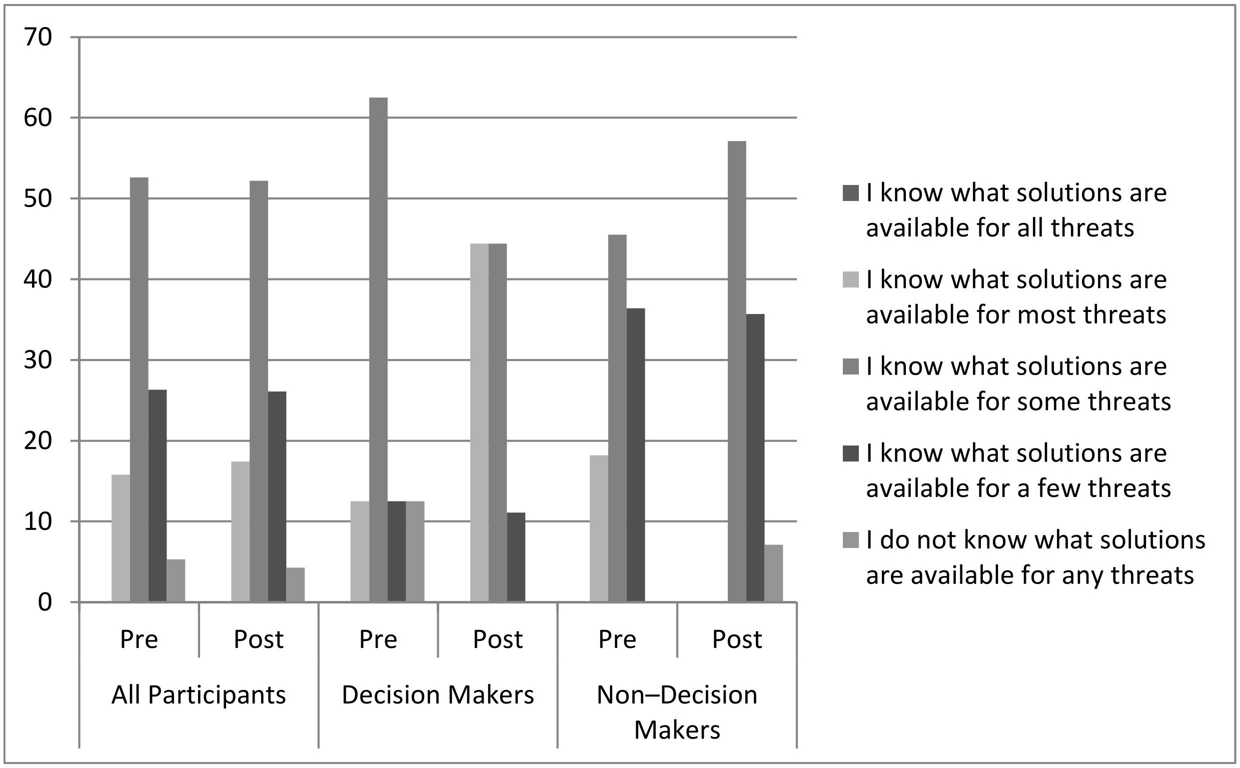
Cyber Security Knowledge

Companies stated that knowledge of cyber security generally increased after participation in the Test Bed, although as they became more aware of cyber security threats and solutions, they also realized the complexity of the situation and in some cases perceived knowledge actually decreased.

The percentage of participants who felt confident their company was aware of when it was being attacked increased from 39.1% to 50.1%. The percentage of companies stating that they knew where to locate information on cyber threats and on potential cyber solutions increased by 5.5% and 5.2%, respectively. Figure 3 provides additional information on companies' stated knowledge of cyber security solutions.

Non–decision makers seemed slightly more confident in their knowledge of available solutions than did decision makers before the Test Bed experience—a higher percentage of non–decision makers than decision makers indicated that they knew what solutions were available for most threats. However, decision makers seemed to increase their perceived knowledge significantly, with approximately 12% expressing that they knew what solutions were available for most threats before the Test Bed, as compared to 44% after the Test Bed. Of note, no respondents believed that they knew what solutions were available for all threats

Figure 3. Knowledge of Available Solutions for Cyber Security Threats



Feedback on the Cyber Test Bed Experience

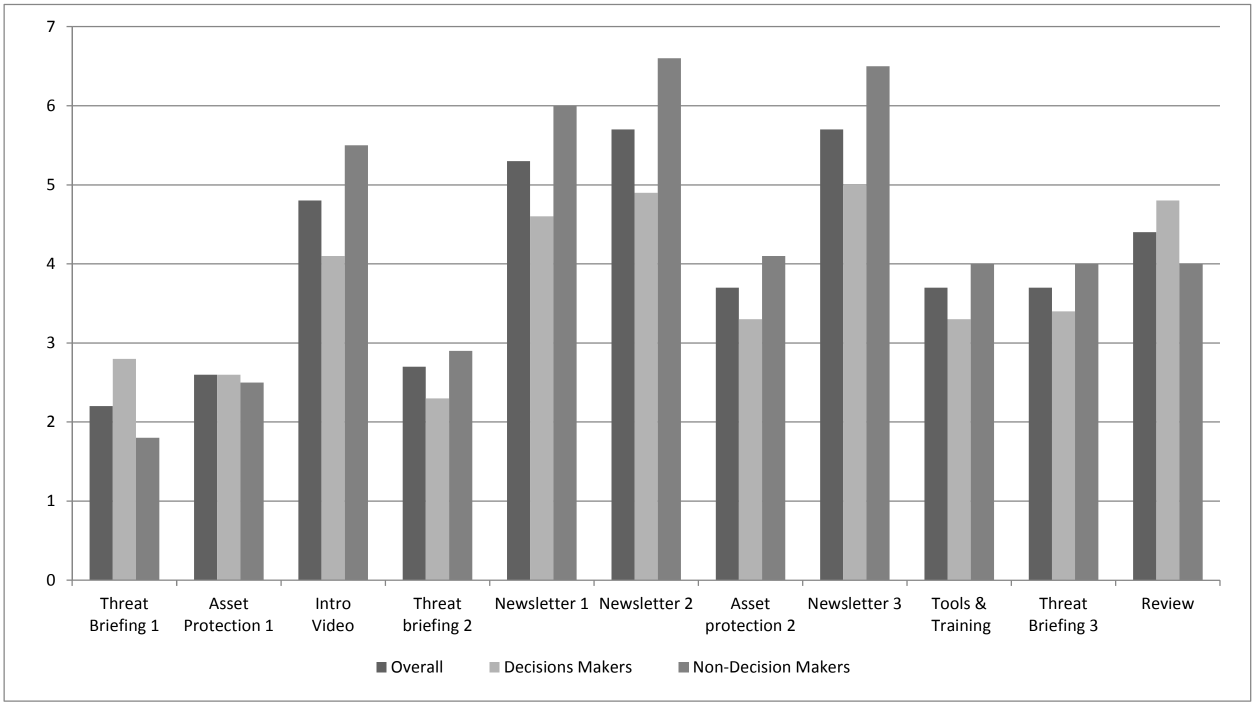
After the Ted Bed experience, we asked participants for feedback. On a scale of 1 to 10 where 1 indicates that the Cyber Test Bed experience was not very valuable and 10 indicates that the Cyber Test Bed experience was highly valuable, the average rating of the Cyber Test Bed experience was an 8. A majority of participants (77.3%) indicated that they would be willing to pay for the Cyber Test Bed, and among those willing to pay, the average amount of money participants were willing to spend was $7,881.30; the responses ranged from $600 to $25,000.

Over 90% of participants indicated they implemented changes recommended by the Cyber Test Bed staff, and over 70% of decision makers indicated that they planned to increase company spending on cyber security in the future.

Most participants (82.6%) indicated that they were surprised by some of the things they learned in the Test Bed, particularly the number and extent of the threats that exist, and all but one of the participants thought other companies, particularly those that deal with online financial transactions or those in the high-tech industry, would benefit from the Cyber Test Bed experience.

Looking at the specific components of the Test Bed experience, the threat briefings and asset protection briefing modules received the highest average ranking among participants. Figure 4 provides a summary of these results (note that lower rankings are better).

Figure 4. Average Rank of Test Bed Modules



General Findings

Given that small and mid-size businesses seemed willing to pay for cyber security training, but have not identified cyber security training that they believe to be worth their money, several potential conclusions could be drawn:

- The quality of existing cyber security training may be insufficient.
- Information on the quality of existing cyber security training may be insufficient.
- The cost of existing cyber security training may be too high.

If the issue is one of insufficient quality or inadequate information on service quality, a role for DHS or another government agency (e.g., NIST) or a private organization may be to help measure/rank the quality of cyber security training providers so that small and mid-size businesses can have an easier time discerning whether the service being offered is worth the price.[2] A government agency could conduct evaluations, or could help to coordinate such evaluations by a private or nonprofit party.

Alternately (or additionally), cyber security training services of sufficient quality may be too expensive for many small and mid-size businesses to afford. If this is the case, government could pay for the development and maintenance of high-quality training materials that cyber security training providers could use. This would save the training providers the money that they would be required to spend to create such materials; some of the savings should flow down to their customers and result in lower prices. Further, cyber security training service providers who use the materials developed by the government might be more easily able to convince small businesses of the quality of their program.

Given the difference in the perceived usefulness of the Test Bed between decision makers and non–decision makers, moving forward, it might not make sense for cyber security training for individuals who are not cyber security decision makers to include information on specific cyber security threats and solutions. Instead, training for these individuals should focus on simple actions that could improve their security, without requiring a significant time commitment. DHS and other government agencies working to develop a strategy to educate small and mid-size businesses on cyber security threats and solutions should be aware of this heterogeneity in the educational needs of small and mid-size business employees.

Broadly, small and mid-size businesses are aware of the need to improve their cyber security, and the Cyber Test Bed project results suggest that training, best practice sharing, and threat analysis are all perceived to be useful. However, small and mid-size businesses are often unable to employee staff dedicated to cyber security, so external resources are needed to support their efforts at increasing cyber security. These resources need to be presented in a way that is easy for staff to understand so that the decision to pay to increase their cyber security (e.g., pay a company offering cyber security training services) is not hampered by lack of information. Further, small and mid-size businesses have different cyber security needs and levels of understanding, and staff within an individual business have very different abilities and levels of need to understand cyber security threats and solutions.

Additional research is needed to investigate what specific types of educational resources benefit small and mid-size businesses the most. This should include a more focused effort at assessing the benefits of specific cyber security training services or tools (e.g., how much companies are willing to pay for), and how these products and services can be presented to companies in such a way that they are able to make decisions and are not hampered by a lack of adequate information (e.g., on the quality of cyber security training services or cyber security tools). For example, a national survey of small businesses could help to provide information on

[2] In economic terms, this suggests that a market failure exists in the market for cyber security training services because *imperfect information* is available to small and mid-size businesses seeking cyber security training services.

how much companies are willing to pay for (a measure of demand) various cyber security training services or tools. A national survey and focus groups of a set of small and mid-size businesses throughout the country could also be used to assess what specific factors affect demand. Such research could help the government identify how they can more effectively and efficiently incentivize increased cyber security investments by small and mid-size businesses through improving information on the quality of products and services or potentially through decreasing the cost of such products and services (e.g., by freely providing and updating robust training resources).

Contact Information

Brent Rowe

114 Sansome St., Suite 500, San Francisco, CA 94104

(415) 848-1317

browe@rti.org

This research brief was prepared by Mr. Brent Rowe, Ms. Katrina Ladd, Ms. Charlotte Scheper, Ms. Cornelia Kaydos-Daniels, Mr. Kemal Piskin, and Ms. Joan Myers.

Brent Rowe, MA, is a Senior Economist at RTI International. He has 10 years of experience studying technology adoption and security related issues and in 2008 coauthored a book titled *Cyber Security: Economic Strategies and Public Policy Alternatives*.

Katrina Ladd, BA, is a Survey Specialist at RTI International. She has previous experience in policy and data analysis and is currently involved with several of RTI's security related projects.

Charlotte Scheper, MA, is the Cyber Security Program Director in the Research Computing Division of RTI International. She has more than 20 years of experience developing tools and methods for ensuring system reliability and security and data integrity and privacy.

S. Cornelia Kaydos-Daniels, PhD, is a Senior Epidemiologist and Director of RTI's Health Security Program. She conducts quantitative and qualitative research on emergency preparedness and response.

Kemal Piskin, MIS, Sec+, is a Senior Cyber Security Engineer at Applied Research Associates, Inc. He has significant experience in leading and managing cyber security and information assurance projects and research.

Joan Myers, BA, is the Director for Cyber and Special Operations Technologies for Applied Research Associates, Inc. She has extensive executive leadership experience, particularly within education, security, and intelligence.

References

Javelin Strategy and Research. (2011). 2011 Small Business Owners (SMBO) Identity Fraud Report: How SMBO Fraud Rates Impact FI Revenues and Retention.

Small Business Administration (2011). Frequently Assessed Questions. Retrieved from http://www.sba.gov/sites/default/files/sbfaq.pdf.