Institute for Homeland Security Solutions

Applied research • Focused results

Cyber Security Test Bed: Summary and Evaluation Results

Final Report

October 2012

Prepared for

Kristina Dorville
National Protection and Programs Directorate
U.S. Department of Homeland Security

Prepared by

Brent Rowe
Katrina Ladd
Charlotte Scheper
S. Cornelia Kaydos-Daniels
RTI International
3040 Cornwallis Road
P.O. Box 12194
Research Triangle Park, NC 27709-2194

with

Kemal Piskin
Joan Myers
Applied Research Associates, Inc.

RTI Project Number 0212782.000.001

RTI Project Number
0212782.000.001

Cyber Security Test Bed: Summary and Evaluation Results

Final Report

October 2012

Prepared for

Kristina Dorville
National Protection and Programs Directorate
U.S. Department of Homeland Security

Prepared by

Brent Rowe
Katrina Ladd
Charlotte Scheper
S. Cornelia Kaydos-Daniels
RTI International
3040 Cornwallis Road
P.O. Box 12194
Research Triangle Park, NC 27709-2194

with

Kemal Piskin
Joan Myers
Applied Research Associates, Inc.

Table of Contents

Chapter **Page**

List of Figures

Figure **Page**

List of Tables

Table **Page**

Executive Summary

ES1. 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. 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).

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.

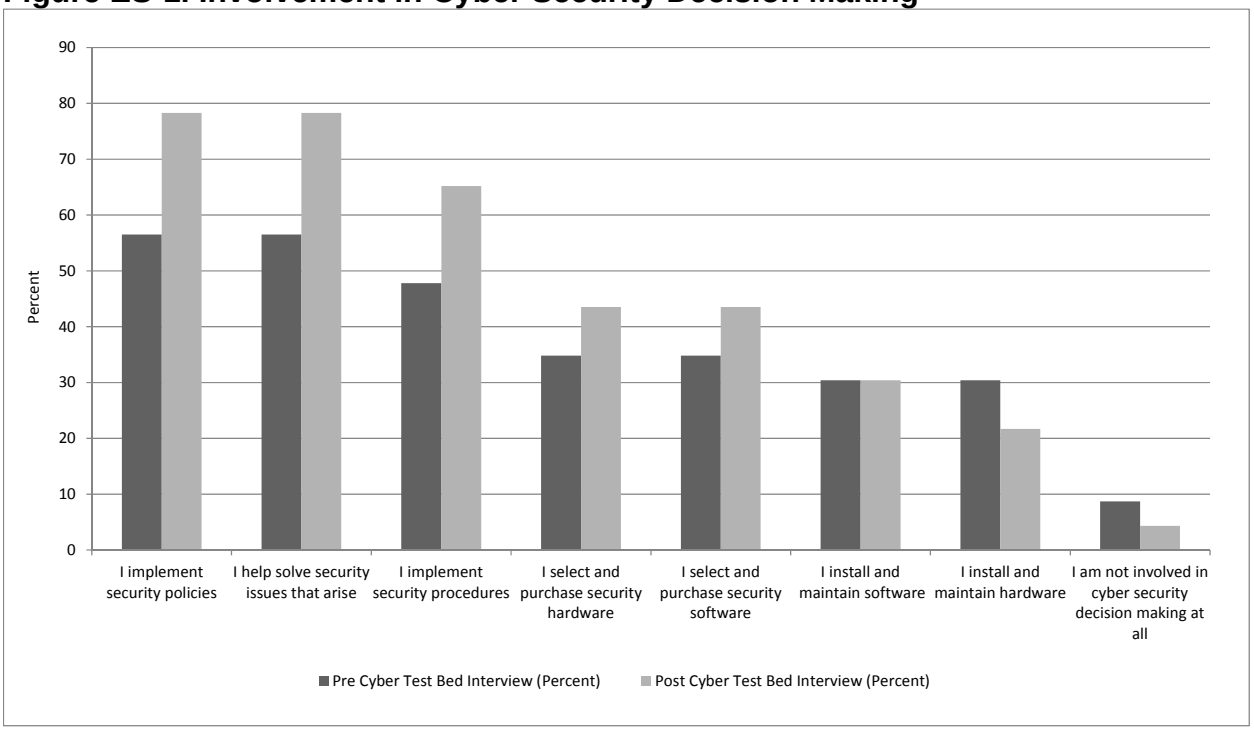
The data we collected and the results of the subsequent analyses provide a useful case study of how a set of cyber security educational tools can have an impact on a set of small businesses. The results

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.

ES2. 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 ES-1. Involvement in Cyber Security Decision Making



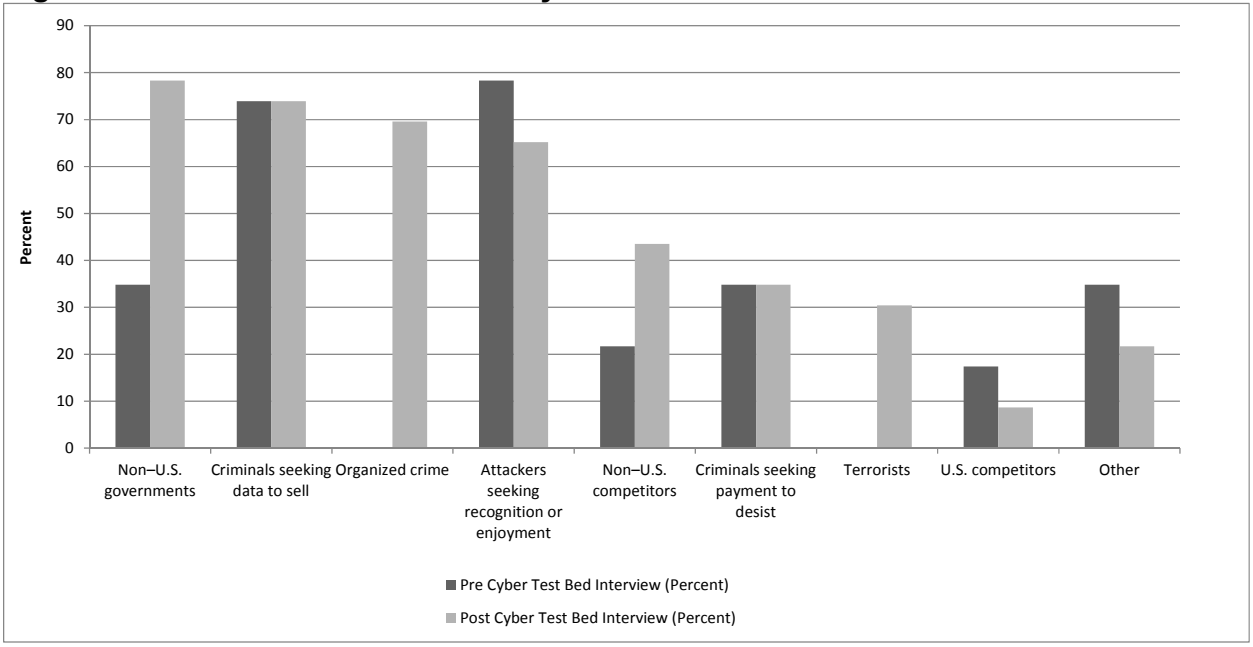
ES3. Cyber Security Perceptions

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 ES-2. Potential Sources of Cyber Attacks



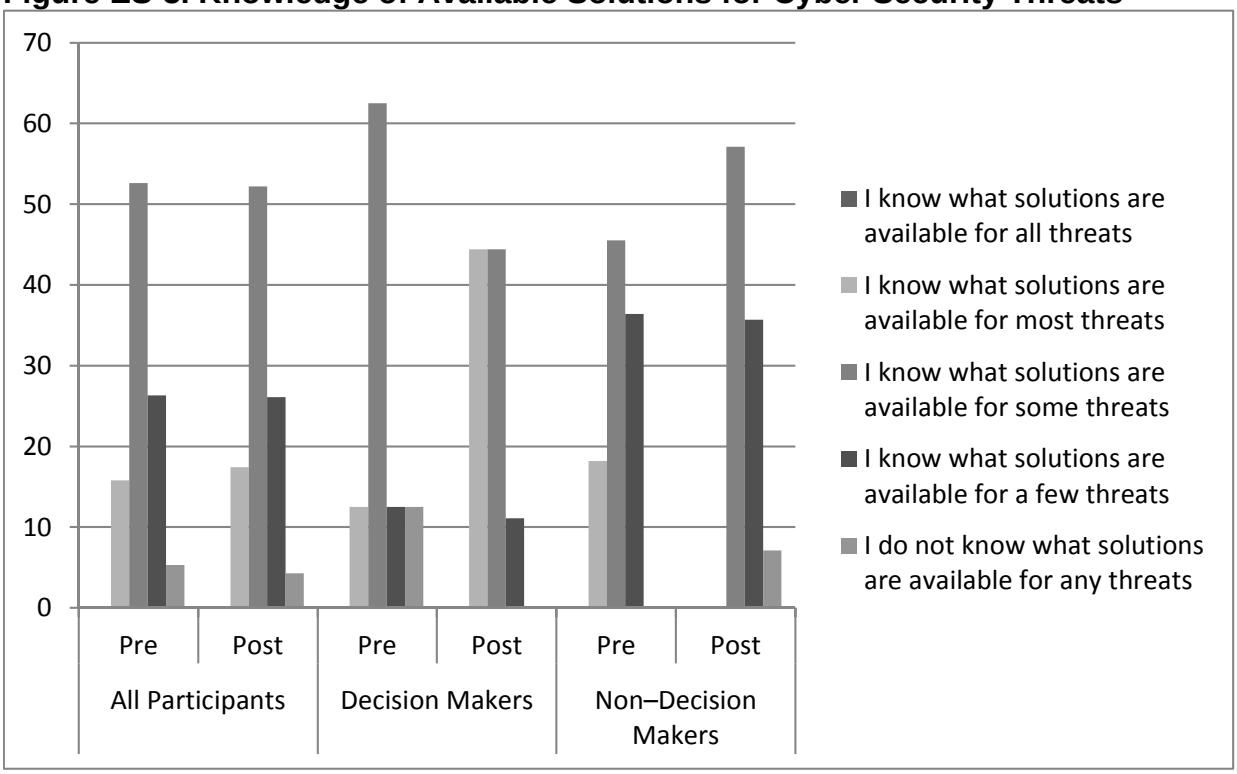
ES4. Cyber Security Knowledge

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 ES-3. Knowledge of Available Solutions for Cyber Security Threats



ES5. Feedback on the Cyber Test Bed Experience

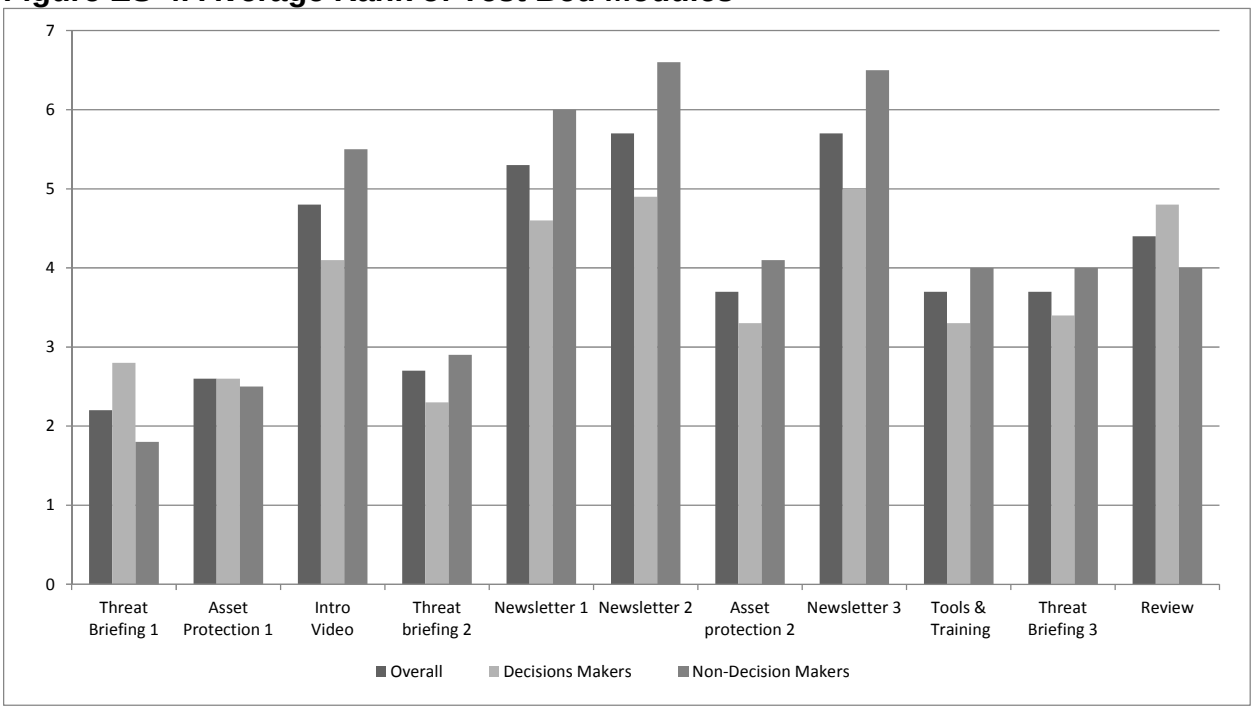
After the Ted Bed experience, we asked participants for feedback. On a scale of 1 to 10 where 1 indicates that the Cyber Test Bed experience was not very valuable and 10 indicates that the Cyber Test Bed experience was highly valuable, the average rating of the Cyber Test Bed experience was an 8. A majority 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 ES-4. Average Rank of Test Bed Modules



ES6. 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.[1] 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

[1] 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.

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 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).

1. Introduction

Although large U.S. businesses and the federal government have made and are continuing to make cyber security investments, small and mid-size companies, which comprise the majority of U.S. private sector organizations, have not done so and their level of cyber security is a concern both for the individual companies' financial health and for the impact their weaknesses could have on supporting intrusion or harm into critical infrastructure.[2] It is critical that private sector companies increase their understanding of cyber threats and put in place the necessary measures to prevent and mitigate future cyber attacks. The Department of Homeland Security (DHS) plays a key role in accomplishing this improved cyber security posture in the private sector. This report describes the results of a DHS-funded project called the Cyber Security Test Bed Project (or the Cyber Test Bed) aimed at increasing the level of understanding of the state of cyber security knowledge, perceptions, and behaviors of small and mid-size businesses. The solutions and training activities tested within the Cyber Test Bed offer specific ways in which DHS and other private and public organizations could provide support for U.S. organizations to increase their cyber security.

The Cyber Test Bed set up 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—for each company, the Cyber Test Bed team extracted and generalized threat data and collected information on cyber security infrastructure (hardware, software, policies, and procedures). Subsequently, the 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.

As part of the evaluation of 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.

This report provides a short summary of the primary Cyber Test Bed components (Section 2), describes the evaluation methodology (Section 3), and describes the results from the evaluation (Section 4). Section 5 reviews key findings and recommends future research directions.

[2] According to a 2011 study by Javelin Strategy and Research , the impact of data and identify theft aimed at small and medium businesses was approximately $8 billion in 2010, with approximately $5.4 billion in losses being borne by small and medium businesses (see https://www.javelinstrategy.com/brochure/209). Losses and costs resulting from the inadequate cyber security of these businesses, which represent over 99% of U.S. companies (see http://www.sba.gov/sites/default/files/sbfaq.pdf), have an impact on not only these businesses but also on their customers, clients and partners, which comprise all U.S. individuals and organizations.

2. Cyber Test Bed: Summary

2.1 Cyber Test Bed Participants

Between November 2010 and April 2011, companies were recruited to participate in the Cyber Test Bed. The original sample of companies to approach about participation was developed by several primary means. First, only businesses in North Carolina were identified, so that travel and other costs could be reduced based on proximity to the project team. Second, the project team members developed the list based on their own contacts, so that recruitment could be expedited. Finally, the total sample of companies to approach was identified with a goal of having some diversity in terms of three primary factors: size (within the set of businesses with fewer than 500 employees), location (within the state of North Carolina), and industry.

More than 65 companies were considered and evaluated for participation. Of those companies, 13 were selected for recruitment into the project. In each case, obtaining an initial meeting was fairly easy. During initial and follow-up recruitment meetings we observed that none of the potential participants felt they were targets or potential victims, and that they were naturally unsure of the "return on investment" of the Test Bed for their business. Although business owners generally knew about high-profile cyber threats or events through media sources, they felt as though security was more of a problem for large businesses, businesses engaged in national defense, or businesses working on complex technology development. Despite these initial reservations, most companies were eager and enthusiastic to sign up and contribute their time to the Test Bed. Approximately 90% of the businesses we approached (banks excluded) initially indicated interest in participating in the process once they were briefed on the intent of the program and its potential value.

In the course of speaking with the executive leadership of certain companies, including small banks and credit unions, company executives (e.g., CEOs, CISOs, and CFOs) were generally very interested in getting an unbiased look at their security. However, obtaining their boards' approval to participate was not possible because their board of directors felt that they already had a sufficient amount of security auditing taking place within their companies.

After several months of recruitment, nine companies agreed to participate. Table 1 provides a general overview of the companies that participated in the Test Bed.[3]

2.2 Cyber Test Bed Components

The overall Test Bed methodology is based on a security model incorporating asset awareness and associated relationships and a process to protect assets and mitigate risk. This process is in turn based on a counterintelligence perspective for identifying and assessing cyber security vulnerabilities. It identifies and mitigates risk through three principal means: (1) increased sensitivity to the threat environment and increased understanding of the corporate assets that may be threatened; (2) practical steps for risk mitigation, including the specification of appropriate user behaviors; and (3) promotion of a policy framework that creates a culture of accountability and provides strong disincentives for ignoring

[3] All of the companies listed below signed a Memorandum of Agreement/Nondisclosure Agreement prior to participation in this project.

threats or contributing to risk. To implement this methodology, the Cyber Test Bed used four core components: (1) threat briefings, (2) threat identification and mitigation tools, (3) training, and (4) a policy framework and protocols.

Table 1. Summary of Cyber Test Bed Participant Companies (2011)

Company Code Name	Location	Estimated Number of Employees	Estimated Annual Revenue, $	Overview
Beeswax	North Piedmont, NC	160 employees	10 million	Business law firm providing counsel to large domestic and foreign private sector clients.
Cedar	South Piedmont, NC	125 employees	20 million	Full-service information technology firm providing technology solutions to its clients.
Coral	South Piedmont, NC	50 employees	15 million	Full-service commercial real estate firm with clients ranging from startups to multinational Fortune 500s.
Curacao	North Piedmont, NC	50 employees	5 million	Venture capital firm invested in more than 100 private companies.
Honeysuckle	Mountains, NC	20 employees	7 million	Private not-for-profit organization providing hands-on educational and research opportunities for science, technology, engineering, and math users.
Lavender	North Piedmont, NC	24 employees	5 million	High-tech private company producing and marketing semiconductor materials.
Peony	North Piedmont, NC	1 employee	100,000	Independent IT services consultant using wireless networking and RFID technology to provide customers with inventory location and tracking.
Phlox	North Piedmont, NC	75 employees	17.5 million	Not-for-profit telecommunications organization providing television and Internet services for hospitality, healthcare, and multidwelling unit properties.
Silver	Mountains, NC	100 employees	5 million	Prefabrication construction company with customer bases in both the public and private sectors.

After identifying a set of potential resources by reviewing existing security technologies, standard policies and procedures, and consulting experts that could be used for each of the components the Test Bed, specific resources were identified for each small business based on its individual needs. The following subsections describe each of the core components in more detail. The complete set of Test Bed materials is included in Appendix A.

2.2.1 Threat Briefings

Three threat briefings were provided to achieve the Test Bed goal to provide timely, actionable intelligence to corporate leaders to help them better understand the threat environment. The first briefing was in conjunction with recruitment and with the development of incentive models and proactive motivators. The second and third threat briefings occurred during the selection and testing of specific technologies within the Test Bed companies.

Key elements of the briefings included information on the following components of a mature organizational cyber security framework:

- Reporting structure and process for all incidents and concerns within the company
- Recognizing insider threat potential
- Understanding the foreign threat potential
- Understanding cyber terrorists
- Integration of counterintelligence/security protocols with information technology (IT) processes, procedures, and protocols
- Connecting with valued partnerships and information sources
- Linking threat environment, actions, and procedures to policies and decision framework for small companies
- Relating corporate motivations to an effective commercial counterintelligence

The threat briefings provided knowledge on current asymmetrical threats, explanation of the cascading or second- and third-order effects of an exploited vulnerability, and a measure of "how could this/would this affect me" in terms of company/self/critical infrastructure (if appropriate). They included real-life examples and other content relevant to the target audience. Briefings also mapped a set of simple strategies to incentivize at least minimal adoption of recommended practices.

2.2.2 Threat Identification and Mitigation Tools

Each of the Test Bed companies had a baseline level of cyber security tools in place, including firewalls, virus detection, incident response mechanisms, and other measures. The Test Bed used a set of state-of-the-art tools that complemented companies' security infrastructure. These tools provided a more robust analysis of intrusions, and asset understanding, context, and relationship mapping.

The two primary tools used were MIR[4], innovative technology to detect and respond to threats within an organization at scale within an enterprise, and Cyber Counterintelligence System for Asset Relationships (CCSAR), a tool to identify relationships to the network, illuminate counterintelligence

[4] http://www.mandiant.com/products/platform/

vulnerabilities, and provide a visual map of assets and relationships. Additional tools such as Snort™[5] and GFI LanGuard™[6] were deployed to assess other asymmetrical threats.[7] The Cyber Test Bed staff also contracted with Mandient®, a company that specializes in deeper scanning to identify Advaced Percsistent Threat (APT) which other network security tools may not find. Because the interactions were with small businesses, the Test Bed team used tools that were low or no cost to use. The Test Bed team was careful not to make specific purchase recommendations; however, the team did provide information on the tools used to perform the vulnerability assessments.

2.2.3 Training

We conducted three rounds of training. Key personnel as determined by the corporate leadership were trained in each company. The training included counterintelligence or security integration concepts, policy formation, communication strategies, outreach, and overall program components. We focused training on the following areas:

- Baseline asset protection and security fundamentals
- Core standards and supporting policies
- Inside/outside threat awareness
- Second- and third-order effects

In all rounds of the training, a variety of subject matter experts in these various areas provided input for and review of curriculum development. Fortalice,[8] a risk, fraud, and security consulting firm run by a former Chief Information Officer in the Executive Office of the President for the White House, was particularly essential in this role.

2.2.4 Policy Framework and Protocols

Although companies may have robust security measures in place, they often do not have protocols or policy frameworks for dealing with intrusions, attacks, or compromises. The Test Bed reviewed existing policy infrastructures and recommended policy frameworks and protocols for each company. The framework started with the decision-making level of the company and focused on the need to create an integrated set of protocols in the five areas of a comprehensive counterintelligence program (physical security, people security, cyber security, intellectual property protection, and contingency planning) to protect the network ecosystem. Applied Research Associates (ARA) used subject matter experts in this area, including Chris Swecker Enterprises (led by the retired Assistant Director Criminal Division of the FBI and the former head of Global Security for Bank of America). In addition, Fortalice delivered a standards framework and policy construct for companies to use. This set of policies provided

[5]Snort™ is an open source network Intrusion Prevention and Detection System (IDS/IPS) that is free to use and community supported. For more information visit http://www.snort.org.

[6] LANGuard™ is a network security and vulnerability scanner that provides a security overview for Microsoft® based computer systems. For more information visit http://www.gfi.com/network-security-vulnerability-scanner.

[7] The CTB performed a number of network vulnerability scans using tools readily available and cost effective for small businesses to use; Snort® and LANGuard™ were two of the tools.

[8]See more information at http://fortalicesolutions.com/

a template that included an acceptable use policy and ethics policy, as well as wireless usage policies and well as reporting criteria for security incidents.

2.3 Cyber Test Bed Outreach Summit

In May 2012, ARA, RTI International, and the Institute for Homeland Security Solutions hosted a conference to provide North Carolina executives with the opportunity to learn more about cyber security and best practices from the Cyber Test Bed. The purpose of the Cyber Security for Executive Leadership conference was to share Cyber Test Bed results and observations with the larger business community, specifically targeted to senior corporate executives. The conference did not intend to teach or discuss the "bytes and code" of cyber security, but rather focused on practical and tactical information that will help businesses in their risk analysis, decision making, and strategic planning.

A total of 105 attendees participated in the conference, including representatives from the region's various private and public industries and from state government entities. The conference also included representatives from a few Fortune 500 companies and participating companies from the Cyber Test Bed. The conference included opening remarks from U.S. Congressman David Price. The conference also included remarks from DHS representative Carlos Kizzee, who addressed proactive cyber security strategies that corporate leaders could use. The conference concluded with discussion from cyber security experts, providing executives with a briefing on several cyber security tools.

3. Evaluation Methodology

To assess the impact of the Test Bed experience, employees at each of the nine companies were interviewed before and after participating in the Test Bed. Twenty-three individuals participated in both phases of data collection, with at least two participating from each company during each phase. The employees participating in the interviews were generally management and executive-level staff members. Originally, the study team aimed to collect information from average staff members to ascertain their cyber security knowledge, perceptions, and behavior and compare these metrics to management executive-level responses; however, soliciting their participation was much more difficult than anticipated. Participating companies were reluctant to agree that average employees could spend the time to take part in the interview process. As such, data collection generally focused on staff in management or executive positions within the company.

3.1 Pre-Intervention Assessment

Prior to each company's participation in the Test Bed, the RTI team conducted interviews with at least two employees at each company. The interview instrument used can be found in Appendix B. The interview focused on several key areas:

- Cyber security perceptions
- Cyber security knowledge
- Cyber security behaviors
- Cyber security needs

This interview instrument included questions for executive/management/IT staff, and questions for "regular staff"; however, only one company allowed regular staff to participate in the interview data collection. As such, the data collected from these staff were not included in the study analysis.

3.2 Post-Intervention Assessment

After each company's participation in the Test Bed, the RTI team conducted interviews with at least two employees at each company. The interview instrument used can be found in Appendix C. The interview instrument included many of the same questions included in the interviews conducted before Test Bed participation; however, several questions were removed that were not expected to change, and several new questions were added that focused on the Cyber Test Bed experience itself. The types of questions asked about:

- Cyber security perceptions
- Cyber security knowledge
- Cyber security behaviors
- Cyber security needs
- Cyber Test Bed experience

3.3 Test Bed Observations

During the Test Bed experience, information was documented on participants' responses. The following broad categories of information were collected by staff managing the Test Bed experience at the nine participating companies:

- How difficult was it to get management buy-in for the Test Bed activities?
- What Test Bed components did the companies/individuals push back on in particular? How did regular staff react when they were included?
- Where did the biggest "ah-ha" moments occur?
- What other key results/takeaways were observed at each company?

This information was noted and catalogued for later analysis.

3.4 Analysis Methodology

Data collected from companies before, during, and after participation in the Test Bed were analyzed mainly by looking at summary statistics and thematic analysis of qualitative information. Given that only 23 individuals participated in interviews from nine companies, the results should be viewed as case study data from a diverse set of small and mid-size North Carolina businesses that provide insight into small and mid-size businesses' knowledge, perceptions, and behaviors regarding cyber security and how an experience such as the Test Bed could change their knowledge, perceptions, and behaviors.

Our analysis first focused on analyzing the data for which respondents were asked to provide ordinal responses. The following analysis steps were undertaken:

- develop summary statistics of key interview question responses, including participant demographics and questions relating cyber security to perceptions and behaviors;
- compare responses by looking at the difference in responses between self-identified cyber security decision makers and non–decision makers; and
- compare responses by looking at questions asked both before and after the Test Bed experience to identify potential changes.

Given the size of the data set, no attempt was made to assess potential correlation between any question responses across participants. Instead, comparisons are made by looking at the average responses from decision makers versus non–decision makers and from company participants before and after the Cyber Test Bed experience.

Additionally, we used thematic analysis to review both information collected during the Test Bed experience and responses to the open-answer questions included in the interviews. Six questions included in the interviews conducted before the Test Bed and five questions included in the interviews conducted after the Test Bed were free form. All of the answers provided by interview participants were typed up, entered into Microsoft Excel, and summarized based on a coding scheme developed by the team; through this process, themes were identified in the responses to questions.

3.5 Pre- and Post-Test Bed Interviews: Sample Demographics

Of the 23 individuals who were interviewed before and after the Cyber Test Bed, 9 self-identified as the primary cyber security decision maker or primary approver of cyber security investments at their company.[9] Fourteen of the participants indicated that they were not the primary decision maker regarding cyber security investments. Table 2 provides a breakout of the sample sizes for each of the overall, decision maker, and non–decision maker categories.

Table 2. Sample Sizes for Overall, Decision Maker, and Non–Decision Maker Categories

Category	Sample Size (n)
All Participants	23
Decision Makers	9
Non–Decision Makers	14

In some cases, participants chose not to a respond to a particular question during the interviews before or after the Test Bed. As a result, the sample size used in some pieces of the following data

[9] This determination was made based on two questions in the interview guide. One asked their role, and one asked who (what role at the company) was the primary decision maker for cyber security investments.

analysis may differ slightly from the sample size outlined in Table 2. In such instances, the revised sample size is noted.

The percentages listed in the data tables refer to the percentage of participants in a sample size who selected a particular response. For example, as displayed in Table 3, 4.3% of the 23 participants in the overall category selected the CIO response option in the pre-Test Bed interviews. Although certain questions allowed for more than one answer, the percentages displayed in the tables below refer to the percentage of the sample size who selected a particular response option.

Table 3. Participants' Role at the Company

Category	Percent (%)					
	All Participants		Decision Makers		Non–Decision Makers	
Interview	Pre	Post	Pre	Post	Pre	Post
Sample Size (n)	23	23	9	9	14	14
CIO	4.3	13.0	0.0	22.2	7.1	7.1
CTO	4.3	4.3	11.1	11.1	0.0	0.0
CFO	13.0	13.0	0.0	0.0	21.4	21.4
President/CEO	26.1	26.1	55.6	44.4	7.1	14.3
Partner/Managing Partner	17.4	17.4	11.1	11.1	21.4	21.4
Head of IT	8.7	13.0	11.1	22.2	7.1	7.1
Controller	4.3	4.3	0.0	0.0	7.1	7.1
VP	8.7	8.7	11.1	11.1	7.1	7.1
Director	8.7	13.0	0.0	11.1	14.3	14.3
Manager	4.3	4.3	0.0	0.0	7.1	7.1
Other/IT Staff	0.0	8.7	0.0	0.0	0.0	14.3

The analysis refers to Question 1 "What is your role at your company?" and Question 4 "Who is the primary decision maker (or final approver) regarding cyber security investments?" in the Pre-Test Bed and Post-Test Bed Interview Guides.

In five cases, the participant's role, decision maker status, or both differed between the pre- and post-interviews. The number of participants indicating that they were a CIO and a decision maker, for example, increased by 22.2% from the pre- to the post-interview. Additionally, although the number of presidents/CEOs remained the same between both interviews, the number of participants who reported they were both the president/CEO and a decision maker decreased from 55.6% in the pre-interview to 44.4% in the post- interview. The changes in company role between the before and after Test Bed interviews may be partly because participants felt that they filled multiple roles listed in the response options. Because the participants work for small business, they may have selected multiple roles before and after the Test Bed to adequately describe the variety of responsibilities encompassed by their position. Table 3 provides the breakout of roles for all interview participants.

Several types of demographic information were collected from the participants during the interviews conducted before the Test Bed. They are presented here for sample description purposes only. No attempt was made to analyze how these data affected other responses to interview questions.

All of the individuals who participated in this study (100%) indicated that their race/ethnicity was white. The average age of participants was 47.04 years and a majority (96.1%) had a bachelor's degree or higher. Table 4 provides a breakdown of the average age among all participants and among those who were decision makers and those who were not decision makers. Table 5 includes a breakdown of the highest levels of education achieved by all participants in the Test Bed study.

Table 4. Average Age of Participants

Category	All Participants	Decision Makers	Non–Decision Makers
Sample Size (n)	26	12	14
Average	47.04	47.25	46.86
Variance	84.92	61.84	110.90

Table 5. Highest Level of Education Achieved by Participants

Category	Percent (%)		
	All Participants	Decision Makers	Non–Decision Makers
Sample Size (n)	26	12	14
Some high school	0.0	0.0	0.0
High school diploma	0.0	0.0	0.0
Associates degree	0.0	0.0	0.0
Some college	3.8	0.0	7.1
College degree	38.5	50.0	28.6
Master's degree	26.9	16.7	35.7
Doctoral degree	19.2	33.3	7.1
Professional degree (e.g., JD, MBA)	11.5	0.0	21.4

4. Qualitative Results: Observational Findings

The following section highlights observational findings regarding cyber security behaviors, policies, knowledge, and information needs and general feedback provided by several participants in the Test Bed experience.

Responses from participants before and after the Test Bed indicate changes in cyber security behaviors. The percentage of time participants spent on cyber security increased after the Test Bed (1.78% to 4.89%) as did the percentage of participants involved with implementing cyber security

policies (56.5% to 78.3%) and cyber security procedures (47.8% to 65.2%) at their companies. However, participants' descriptions of the IT decision-making processes in place at their companies did not change after the Test Bed.

Responses from participants regarding cyber security perceptions also changed in some instances after the Test Bed. The percentage of participants reporting documented policies, access restrictions, and employee training in place for cyber security, intellectual property security, and physical security increased largely after the Test Bed. Although participants seemed slightly less concerned about cyber security after the Test Bed, the percentage of participants who felt that their company spent an appropriate amount of time and money on cyber security decreased by 21.7%. Lastly, the percentage of participants who perceived non–U.S. governments and organized crime as potential sources of cyber attacks increased from 34.8% to 78.3% and 0% to 69.6%, respectively.

With regard to cyber security knowledge, participants indicated an increase in the likelihood of experiencing a cyber attack (46.9% to 64.0%) and an increase in the likelihood of being able to detect a cyber attack (39.1% to 50.1%) after the Test Bed. In addition, a higher percentage of participants reported knowing the solutions available for most cyber security threats after the Test Bed (12.5% to 44.4%).

Participants' responses regarding cyber security information needs were mixed. Many participants said they knew more information about cyber security now than before the Test Bed, but they still did not think they had all the information. Suggestions for additional information included regularly updated material on cyber security threats and websites containing cyber security best practices. In addition, participants overwhelmingly cited a security breach or cyber attack as the primary factor that would incentivize them to spend more money on cyber security.

Lastly, feedback from participants on the Cyber Test Bed was generally positive. The Test Bed received an average rating of 8 from participants on a scale of 1 to 10 where 1 indicates the experience was not very valuable and 10 indicates the experience was highly valuable. A majority of participants (77.3%) indicated that they would be willing to pay for the Test Bed. A majority of participants (90.5%) also indicated that their companies had made changes recommended by the Test Bed staff. Lastly, all but one participant thought that other companies, particularly those in the high-tech industry and those that deal with online financial transactions, would benefit from the Cyber Test Bed.

4.1 Cyber Security Behaviors

The following section on cyber security behaviors discusses participants' responses from before and after the Test Bed regarding the amount of time spent on cyber security, the level of involvement in the cyber security decision-making process, and the overall IT decision-making process at each of the Test Bed companies.

Participants in the Test Bed sample vary quite a bit in terms of the amount of time they spend on cyber security. Table 6 summarizes the average time participants spent on cyber security. The average amount of time participants spent on cyber security increased from 1.78% before the Test Bed to 4.89% after. Responses ranged from 0% to 10% before the Test Bed to 0% to 25% after.

This difference between responses before and after the Test Bed experience suggests that companies' perception of the risk of cyber security increased or their perception of their ability to reduce their risk may have increased. Companies may have learned information from the Test Bed that made them more concerned (i.e., increased their view of their cyber security risk). Additionally, or alternately, companies who increased the time they spend on cyber security might have done so because the Test Bed made them feel better informed and thus better able to make more efficient and effective decisions. For example, prior to the Test Bed, an individual company may have felt that its knowledge was so poor that it did not want to invest in cyber security because it did not think that the money would provide a positive return on investment (ROI), but now that it is better informed, it perceives a better ROI on certain investments.

Table 6. Average Percent of Time Spent on Cyber Security by Participants

Category	Percent (%)					
	All Participants		Decision Makers		Non–Decision Makers	
Interviews	Pre	Post	Pre	Post	Pre	Post
Sample Size (n)	23	23	9	9	14	14
Average	1.78	4.89	1.61	2.78	1.89	8.04
Variance	2.77	42.03	6.31	6.07	0.48	57.71

The analysis in Table 6 refers to Question 2 in the Pre- and Post-Test Bed Interview Guides: "How much time do you personally spend on cyber security related activities as a percent of your time?"

Both decision makers and non–decision makers increased the amount of time they spent on cyber security. The percentage of time spent on cyber security by decision makers increased from 1.61% before the Test Bed to 2.78% after. The percentage of time spent on cyber security by non–decision makers increased from 1.89% before the Test Bed to 8.04% after.

The difference in time spent on cyber security between the decision makers and non–decision makers after the Test Bed suggests increased involvement of non–decision makers in cyber security–related issues at their companies. Decision makers were likely already involved in cyber security issues at their company or lacked the additional time to devote to cyber security on a regular basis. The Test Bed may have provided non–decision makers who had little previous knowledge of cyber security with the opportunity to increase their cyber security awareness on a day-to-day basis.

Participants' involvement in cyber security decision making differed somewhat after the Test Bed. Overall, participants' level of involvement in the cyber security decision making process increased or stayed the same for six of the eight items listed in Table 7. Participants' level of involvement in implementing security policies and helping to solve security issues that arise increased by the largest amount (21.8%) after the Test Bed. Participants' involvement in implementing security procedures increased by the second largest amount, from 47.8% before the Test Bed to 65.2% after.

The change in responses among participants before and after the Test Bed suggests that the Test Bed influenced the number and types of people involved in cyber security decision making. For example,

after completing the Test Bed experience both decision makers and non–decision makers may be more aware of ways in which they can become involved in implementing security policies and procedures at their company and in solving security issues that arise. An increase in the number of individuals involved in various components of the cyber security decision-making process suggests that the Test Bed helped engage more participants in the cyber security decision-making process.

Table 7. Participants' Involvement in Cyber Security Decision Making

Category	Percent (%)					
	All Participants		Decision Makers		Non–Decision Makers	
Interview	Pre	Post	Pre	Post	Pre	Post
Sample Size (n)	23	23	9	9	14	14
I select and purchase security hardware	34.8	43.5	44.4	55.6	28.6	35.7
I select and purchase security software	34.8	43.5	44.4	55.6	28.6	35.7
I install and maintain hardware	30.4	21.7	33.3	22.2	28.6	21.4
I install and maintain software	30.4	30.4	33.3	22.2	28.6	35.7
I implement security policies	56.5	78.3	55.6	88.9	57.1	71.4
I implement security procedures	47.8	65.2	33.3	55.6	57.1	71.4
I help solve security issues that arise	56.5	78.3	66.7	100.0	50.0	64.3
I am not involved in cyber security decision making at all	8.7	4.3	11.1	0.0	7.1	7.1

The analysis refers to Question 3 in the Pre- and Post-Test Bed Interview Guides: "What is your involvement in cyber security decision making?"

Participants' descriptions of the IT security decision-making process varied across companies. There appear to be two IT security decision-making processes within the Test Bed sample: a process that takes place internally within the company and one that is outsourced to an outside IT consultant/contractor. The six companies that described an internal decision-making process discussed the roles that employee collaboration and a positive cost-benefit analysis play in making final IT decisions. The three Test Bed companies that relied on an outsourced vendor for IT support discussed the important role that recommendations from the IT consultant/contractor plays in making final IT-related decisions.

There did not appear to be significant impact from the Test Bed on the IT decision-making process as participants' descriptions of the processes at their companies were similar before and after the Test Bed. However, two participants noted that, since taking part in the Test Bed, the IT decision-making processes at their respective companies has become more collaborative and grown to include inputs from a greater number of employees and another participant noted that after completing the Test Bed, his company would now be building cyber security into its strategic plan.

Regarding cyber security behaviors, responses from participants after the Test Bed indicated an increase in the amount of time spent on cyber security and an increase in implementing security policies and procedures and resolving security issues. However, responses from participants after the Test Bed did not suggest a change in the cyber security decision-making process at their companies.

4.2 Cyber Security Perceptions

Companies' cyber security perceptions comprise the way in which they view cyber security threats and solutions, and the level and value of each. The interviews and observational data helped the Test Bed team assess the cyber, intellectual property, and physical security policies participants perceived to be in place at each of their companies. Participants' cyber security concerns and their perceptions of the appropriateness of company spending on cyber security were also queried.

The policies in place for cyber, intellectual property, and physical security varied slightly among companies and participants. Tables 8, 9, and 10 summarize the cyber, intellectual property, and physical security policies that participants perceived or understood were in place at their company. The presence of cyber, intellectual property, and physical security policies was not objectively verified. The percentage of companies with documented policies, access restrictions, and employee training in place for cyber, intellectual property, and physical security increased or stayed the same after the Test Bed for seven of the nine Test Bed companies. The percentage of companies with documented policies in place for intellectual property security decreased from 64.3% before the Test Bed to 35.3% after. Similarly, the percentage of companies with access restrictions in place for physical security decreased from 100% before the Test Bed to 94.1% after.

The increase or continued use of most cyber, intellectual property, and physical security policies after the Test Bed suggests that the Test Bed had a positive impact on cyber security policies within participating companies. The Test Bed, for example, may have drawn attention to the need for written and formal security policies. Of note, in one case the percentage of companies with policies in place related to cyber security decreased; fewer non–decision makers reported having a documented cyber security policy after the Test Bed than before. Non–decision makers may not be as well informed of the existence, or lack thereof, of documented policies, which tend to be more the purview of management (decision makers). Non–decision makers may also now have a better understanding of what constitutes a policy, and now recognize that no policies were originally in place at their company. Each participant was provided with a collection of security policies that covered multiple security aspects and could easily be implemented or tailored to their specific needs. This security policy package was received with a great deal of positive feedback.

The contingency plans participants perceived or understood to be in place at the Test Bed companies varied quite a bit before and after the Test Bed. Table 11 summarizes the responses from participants, decision makers, and non–decision makers regarding company contingency plans. Prior to the Test Bed, all participants (100%) indicated that their companies had contingency plans in place for situations such as loss of power and network connectivity. After the Test Bed, this number dropped to 86.4%. A decrease in contingency plans was also seen in responses for both decision makers and non–decision makers.

Table 8. Policies in Place for Cyber Security

Category	Percent (%)					
	All Participants		Decision Makers		Non–Decision Makers	
Interview	Pre	Post	Pre	Post	Pre	Post
Sample Size (n)	18	18	8	8	10	10
Documented policies	38.9	55.6	25.0	75.0	50.0	40.0
Access restrictions	100.0	100.0	100.0	100.0	100.0	100.0
Employee training	55.6	66.7	50.0	75.0	60.0	60.0
Other	5.6	5.6	12.5	0.0	0.0	10.0
None	0.0	0.0	0.0	0.0	0.0	0.0

This analysis refers to Question 6 in the Pre- and Post-Test Bed Interview Guides: "For each of the following types of security, please indicate any policies/procedures that you have in place."

Table 9. Policies in Place for Intellectual Property Security

Category	Percent (%)					
	All Participants		Decision Makers		Non–Decision Makers	
Interview	Pre	Post	Pre	Post	Pre	Post
Sample Size (n)	17	17	7	7	10	10
Documented policies	64.3	35.3	66.7	42.9	62.5	30.0
Access restrictions	71.4	88.2	66.7	85.7	75.0	90.0
Employee training	50.0	58.8	50.0	57.1	50.0	60.0
Other	0.0	5.9	0.0	0.0	0.0	10.0
None	21.4	5.9	16.7	0.0	25.0	10.0

This analysis refers to Question 6 in the Pre- and Post-Test Bed Interview Guides: For each of the following types of security, please indicate any policies/procedures that you have in place.

Table 10. Policies in Place for Physical Security

Category	Percent (%)					
	All Participants		Decision Makers		Non–Decision Makers	
Interview	Pre	Post	Pre	Post	Pre	Post
Sample Size (n)	17	17	8	8	9	9
Documented policies	72.2	76.5	50.0	75.0	90.0	77.8
Access restrictions	100.0	94.1	100.0	87.5	100.0	100.0
Employee training	72.2	76.5	62.5	75.0	80.0	77.8
Other	0.0	0.0	0.0	0.0	0.0	0.0
None	0.0	0.0	0.0	0.0	0.0	0.0

This analysis refers to Question 6 in the Pre- and Post-Test Bed Interview Guides: "For each of the following types of security, please indicate any policies/procedures that you have in place."

Table 11. Contingency Plans in Place

Category	Percent (%)					
	All Participants		Decision Makers		Non–Decision Makers	
Interview	Pre	Post	Pre	Post	Pre	Post
Sample Size (n)	20	22	8	9	12	13
Yes	100.0	86.4	100.0	88.9	100.0	84.6
No	0.0	13.6	0.0	11.1	0.0	15.4

This analysis refers to Question 7 in the Pre- and Post-Test Bed Interview Guides: "Do you have contingency plans in place (e.g., for loss of power, network connectivity?)."

Although the data suggest that the number of contingency plans in place decreased after the Test Bed, it is unlikely that companies involved in this project removed contingency plans for loss of power and network connectivity. The apparent decrease in contingency plans can be explained by a change in interview participant sample size before and after the Test Bed for this question. Three participants from the same company indicated during the interview after the Test Bed that they did not have contingency plans in place. During the interviews prior to the Test Bed, the same three participants did not respond to the question. The addition of responses from this company during the interviews after the Test Bed explains the decrease in the percentage of companies with contingency plans.

Observationally, during the Test Bed companies learned more about contingency plans and how to adequately implement them. As such, the post-Test Bed data should be viewed as a more accurate assessment of contingency plans in place.

Participants' definitions of cyber security differed only slightly in the before and after Test Bed interviews. In many responses before the Test Bed, participants used the words "protect proprietary or sensitive information," protection of "assets," and prevention of "unauthorized access" to define cyber security. Definitions from after the Test Bed mentioned protection from outside threats more often than responses prior to the Test Bed. For example, before the Test Bed, one participant defined cyber security as "network hardware and software security, both external and internal." After completing the Test Bed, the same participant defined cyber security as "protecting your assets from domestic and foreign threats." The Test Bed may have helped participants broaden their definition of cyber security and align cyber security with asset protection.

Test Bed participants' and companies' level of concern toward cyber security decreased after the Test Bed. Table 12 summarizes the average level of concern toward cyber security among participants, decision makers, and non–decision makers. On a scale of 1 to 10 where 1 means an individual participant is not concerned at all and 10 means that a participant is very concerned about cyber security, on average, respondents indicated a concern level of approximately 5.87 before the Test Bed experience and 5.0 after. Responses ranged from 2 to 10 before the Test Bed and 3 to 8 after. Decision makers and non–decision makers indicated similar levels of concern both before and after the Test Bed. The level of concern indicated by decision makers decreased from 5.89 to 5.1 after the Test Bed. Similarly, the level of concern indicated by non–decision makers decreased from 5.86 to 5.0 after the Test Bed.

Table 12. Participants' Average Level of Concern Toward Cyber Security

Category	All Participants		Decision Makers		Non–Decision Makers	
Interview	Pre	Post	Pre	Post	Pre	Post
Sample Size (n)	23	23	9	9	14	14
Average	5.87	5.0	5.89	5.1	5.86	5.0
Variance	5.03	3.1	5.86	2.7	4.90	3.5

Among all participants, the degree of concern toward cyber security decreased after the Test Bed. In Table 13, data on companies' level of concern were grouped into categories and analyzed pre- and post-Test Bed. For example, the number of participants reporting that they were very concerned about cyber security dropped from 30.4% before the Test Bed to 21.7% after. Similarly, the number of participants reporting that they felt extremely concerned about cyber security dropped from 8.7% to 0% after the Test Bed. The number of participants reporting that they were a little concerned about cyber security increased from 21.7% before the Test Bed to 43.5% after. A decrease in the degree of concern for cyber security is also evident for decision makers and non–decision makers.

Table 13. Participants' Level of Concern Toward Cyber Security: Presented in Categories

Category	Percent (%)					
	All Participants		Decision Makers		Non–Decision Makers	
Interview	Pre	Post	Pre	Post	Pre	Post
Sample Size (n)	23	23	9	9	14	14
Hardly concerned	4.3	0.0	11.1	0.0	0.0	0.0
A little concerned	21.7	43.5	11.1	22.2	28.6	57.1
Somewhat concerned	34.8	34.8	44.4	55.6	28.6	21.4
Very concerned	30.4	21.7	22.2	22.2	35.7	21.4
Extremely concerned	8.7	0.0	11.1	0.0	7.1	0.0

The analysis in Tables 12 and 13 refers to Question 9 in the Pre- and Post-Test Bed Interview Guides: "How worried are you about cyber security on a scale of 1 to 10?" (1= not worried about cyber security, 10= cyber security keeps me up at night).

The difference in responses before and after the Test Bed could mean that the knowledge the Test Bed provided to participants and companies reduced the amount of worry they felt toward cyber security. For example, after the Test Bed, companies may have found that cyber security was not as hard or expensive to achieve as they had previously thought. Companies may have put new policies or technologies in place to monitor cyber security threats, perhaps making participants feel more secure about cyber security at their company. After participating in the Test Bed, companies may now feel that they have the information they need to make informed investment decisions that protect their assets and mitigate cyber security risks.

The type of cyber security concerns of participants also changed slightly after the Test Bed. Table 14 summarizes the relative concern participants had toward loss of data/intellectual property, loss of customers/reputation, productivity loss, and other concerns before and after the Test Bed. Of note, all or almost all interview participants (22 to 23 individuals) provided a first, second, and third ranking in both the pre- and post-Test Bed interviews, but only 4 and 9 individuals provided a fourth-ranked concern in the pre-Test Bed and post-Test Bed interviews, respectively.

Table 14. Summary of Cyber Security Concerns

Category	Percent (%)							
	Rank 1		Rank 2		Rank 3		Rank 4	
Interview	Pre	Post	Pre	Post	Pre	Post	Pre	Post
Sample Size (n)	23	23	23	22	22	22	4	9
Loss of data/ intellectual property	56.5	37.5	21.7	34.8	18.2	18.2	25.0	22.2
Loss of customers/ reputation	21.7	12.5	26.1	17.4	54.5	54.5	0.0	33.3
Productivity loss	17.4	25.0	52.2	43.5	27.3	22.7	0.0	11.1
Other	4.3	25.0	0.0	4.3	0.0	4.5	75.0	33.3

The analysis refers to Question 10 in the Pre- and Post-Test Bed Interview Guides: "What in particular are you concerned about regarding cyber security? (Please Rank)"

Loss of data/intellectual property still remained the primary concern among participants both before and after the Test Bed. Although a majority of participants (56.5%) ranked loss of data/ intellectual property as their primary concern before the Test Bed, this percentage fell to 37.5% after. However, the percentage of participants who ranked productivity losses as their number one concern increased from 17.4% before the Test Bed to 25.0% after. A majority of participants (54.5%) ranked loss of customers/reputation third both before and after the Test Bed.

Although the order of the ranking of cyber security concerns did not change after the Test Bed, the increase in the percentage of participants who ranked productivity loss as their number one concern may highlight the influence the Test Bed had on participants' understanding of the implications of a cyber attack. In addition to the potential loss of data, a greater number of participants also seem to be more aware of the potential loss in productivity resulting from a cyber security threat or attack. By broadening the areas of concern, participants may be able to better establish contingency plans addressing productivity, data, and intellectual property losses.

Responses from participants and companies regarding the appropriateness of the amount of resources spent on cyber security changed after the Test Bed. As summarized in Table 15, the percentage of participants who thought their company spent the appropriate amount of time and money on cyber security decreased from 47.8% before the Test Bed to 26.1% after. Conversely, the percentage of participants who thought their company did not spend the appropriate amount of time and money on cyber security rose from 39.1% to 56.5%. The percentage of participants who indicated that they did not

know whether their company spent the appropriate amount of resources on cyber security also rose by 4.4% after the Test Bed.

Table 15. Appropriateness of Time and Money Spent on Cyber Security

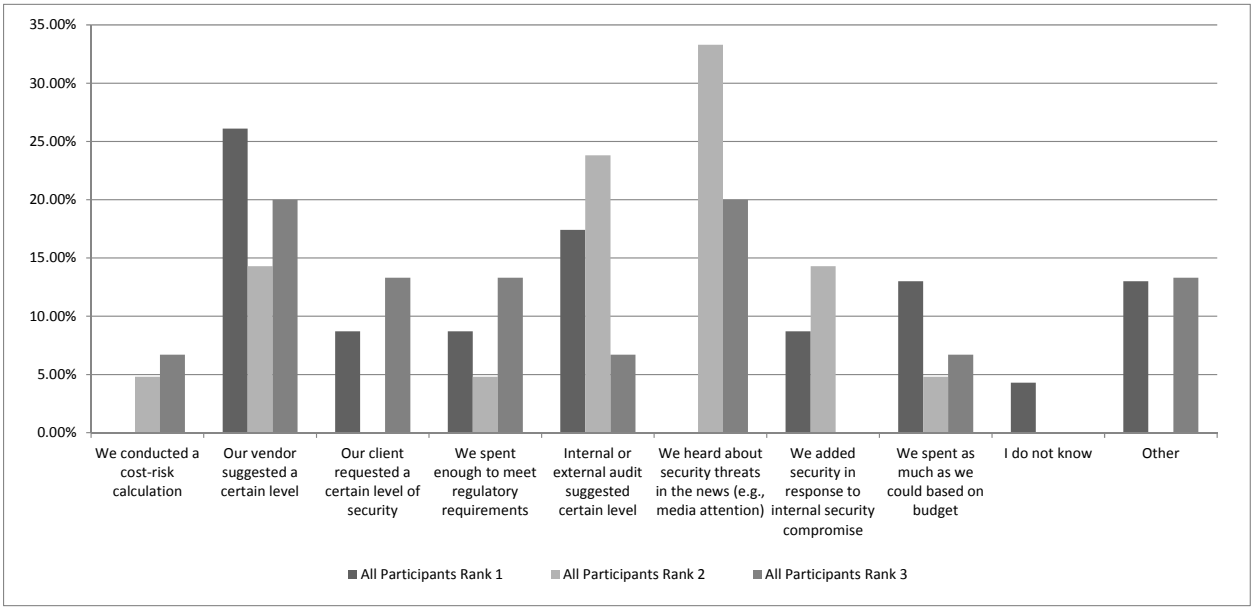
Category	Percent (%)					
	All Participants		Decision Makers		Non–decision Makers	
Interview	Pre	Post	Pre	Post	Pre	Post
Sample Size (n)	23	23	9	9	14	14
Yes	47.8	26.1	44.4	33.3	50.0	21.4
No	39.1	56.5	55.6	66.7	28.6	50.0
Don't Know	13.0	17.4	0.0	0.0	21.4	28.6

This analysis refers to Question 11 in the Pre- and Post-Test Bed Interview Guides: "Do you believe that your company spends the appropriate amount of money and time on cyber security?"

The change in responses among participants before and after the Test Bed experience may suggest that the Test Bed highlighted areas for improvement in how the companies handle cyber security. Before the Test Bed, for example, companies may have thought that they spend an adequate amount of resources on cyber security–related issues. After the Test Bed, however, these companies may have identified additional investment and personnel strategies that would improve cyber security.

Figure 1 summarizes the importance of various factors in arriving at the current level of cyber security spending at companies participating in the Test Bed. These data, as provided by interview respondents, show the items that commonly were ranked as first, second, and third most important factors. The highest percentage of participants (26.1%) ranked "our vendor suggested a certain level" as the number one factor in how their company arrived at its current level of cyber security spending. It is worth noting that participants from three of the four companies that relied on a vendor to determine the appropriate amount of time and money to spend on cyber security also outsourced all of their IT processes. Participants ranked security threats in the news most frequently as the second factor contributing to cyber security spending levels (33.3%), and vendor suggestions and threats in the news were tied as the third factor contributing to cyber security spending (20.0%). In addition to those highlighted above, of note, 17.4% of respondents ranked as first that internal or extra audit information suggested a certain level of security and 13.0% ranked as first that they spend as much as they can based on their budget.

Figure 5. Company Arrival at Current Level of Cyber Security Spending



The analysis refers to Question 12 in the Pre-Test Bed Interview Guide: "How did you arrive at your current level of spending? In the list below, for any factor that affects your cyber security spending, please rank them in terms of their relative importance (beginning with "1" for the factor that most influences your current level of spending on security) and write in any other factors as appropriate." The analysis is based on the following sample sizes: All Participants Rank 1=23, All Participants Rank 2=21, All Participants Rank 3=15.

The responses to the types of sources for cyber security attacks changed after the Test Bed. Table 16 summarizes the changes in responses among participants, decision makers, and non–decision makers. The changes in responses suggest a shift in the sources for potential cyber attacks. Prior to the Test Bed, for example, 78.3% of participants felt that attackers seeking recognition were cyber attacking or might attack their company. This number dropped to 65.2% after the Test Bed. On the other hand, the percentage of participants who felt non-U.S. governments might attack their company increased from 34.8% before the Test Bed to 78.3% after. The percentage of participants who selected organized crime and terrorists as potential sources of cyber attacks increased from 0% to 69.6% and 0% to 30.4%, respectively.

Table 16. Potential Sources of Cyber Attacks

Category	Percent (%)					
	All Participants		Decision Makers		Non–Decision Makers	
Interview	Pre	Post	Pre	Post	Pre	Post
Sample size (n)	23	23	9	9	14	14
U.S. competitors	17.4	8.7	11.1	11.1	21.4	7.1
Non–U.S. competitors	21.7	43.5	44.4	77.8	7.1	21.4
Non–U.S. governments	34.8	78.3	55.6	100.0	21.4	64.3
Criminals seeking data to sell	73.9	73.9	77.8	55.6	71.4	85.7
Criminals seeking payment to desist	34.8	34.8	55.6	33.3	21.4	35.7
Attackers seeking recognition or enjoyment	78.3	65.2	77.8	66.7	78.6	64.3
Organized crime	0.0	69.6	0.0	66.7	0.0	71.4
Terrorists	0.0	30.4	0.0	11.1	0.0	42.9
Other	34.8	21.7	33.3	22.2	35.7	21.4

This analysis refers to Question 16 in the Pre-Interview Guide and Question 13 in the Post-Interview Guide: "Who do you think is attacking (cyber attacking) your company or might attack your company?"

The differences in responses before and after the Test Bed suggest that the content of the Test Bed may have changed participants' perceptions on the likely sources of cyber attacks. As small businesses, many of the companies that participated in this project may have felt that they would not be targeted by non–U.S. governments, organized crime, or terrorists. After completing the Test Bed, participants may now see their intellectual property and data assets as vulnerable to cyber attacks from larger organizations.

The items selected as factors increasing the threat of cyber security did not vary widely before and after the Test Bed. Table 17 summarizes the responses receiving during both sets of interviews for overall participants, decision makers, and non–decision makers. A majority of participants (90.6%) indicated before the Test Bed that common websites (e.g., popular news websites and social network websites) increased the threat of cyber security to their company. A majority of participants (88.9%) continued to view the security of common websites as the top factor in increasing the threat of cyber security to their company.

Open-ended interview question responses suggest that in many cases, participants did not feel their company's downstream customers' or upstream suppliers' levels of IT security affected their IT security decisions. With respect to downstream customers' level of IT security, three respondents from different companies emphasized the importance of ensuring that they and their companies were protected against any breaches in customer security. For example, one participant noted that "Between the start of this program and now we have a downstream client with one of our projects and it's quite possible that

what we're doing could influence them. This causes me to take a little extra precaution in dealing with the instruments and areas of the site that they have access to." Similarly, with respect to upstream suppliers' levels of IT security, participants indicated that they took steps to secure proprietary information and mitigate risk to the company.

Table 17. Factors Increasing the Threat of Cyber Security

Category	Percent (%)					
	All Participants		Decision Makers		Non–Decision Makers	
Interview	Pre	Post	Pre	Post	Pre	Post
Sample size (n)	18	18	8	8	10	10
IT vendors	22.7	22.2	22.2	12.5	23.1	30.0
Suppliers	13.6	22.2	0.0	12.5	23.1	30.0
Customers/clients	31.8	44.4	44.4	37.5	23.1	50.0
ISP	31.8	33.3	55.6	62.5	15.4	10.0
Common websites	90.9	88.9	88.9	87.5	92.3	90.0
Home internet users	77.3	61.1	88.9	50.0	69.2	70.0
Other	50.0	22.2	55.6	37.5	46.2	10.0

This analysis refers to Question 17 in the Pre-Interview Guide and Question 14 in the Post-Interview Guide: "Do you believe any of the following factors/entities are increasing the threat of cyber attacks to your organization?"

Regarding cyber security perceptions, responses from participants after the Test Bed indicated in most cases an increase in the percentage of cyber security, intellectual property, and physical security policies in place at Test Bed companies. Although the average level of concern toward cyber security decreased among participants after the Test Bed, loss of data/intellectual property remained the primary cyber security concern among participants in the interviews both before and after the Test Bed. A higher percentage of participants felt that their companies did not spend an appropriate amount on cyber security after the Test Bed. Lastly, a higher percentage of participants saw organized crime, terrorists, and non–U.S. governments as likely sources of cyber attacks after the Test Bed.

4.3 Cyber Security Knowledge

The following section discusses participants' responses to questions regarding cyber security knowledge, including estimates on cyber security–related losses, the occurrence of cyber security attacks and the ability to detect them, the location of cyber security solution and threat information, and the resources available for cyber security advice.

Estimates from participants on the amount of employee productivity, product delays, and intellectual property lost in 2010 decreased after the Test Bed. Across all categories (overall, decision makers, and non–decision makers), participants' estimates on the amount of money lost were lower after the Test Bed than before. As displayed in Table 18, estimated losses were $30,626 less after the Test Bed than estimates before the Test Bed. It is important to note that these estimates were uneducated guesses and that many participants did not know how to measure these losses. In addition, more time had elapsed

between the interviews before and after the Test Bed but the question did not change. Participants may have forgotten the details regarding losses experienced in 2010.

Table 18. 2010 Cyber Security–Related Losses for Companies in the Test Bed

Category	All Participants		Decision Makers		Non–Decision Makers	
Interview	Pre	Post	Pre	Post	Pre	Post
Sample Size (n)	19	18	9	9	9	10
Average (dollars)	51,237	20,611	89,444	18,888	22,333	16,850
Variance	12,654,315,789	905,192,810.5	24,840,277,778	1,211,111,111.1	454,725,000	705,750,000.0

This analysis refers to Question 34 in the Pre- Interview Guide and Question 17 in the Post- Interview Guide: "How much do you believe your company lost in terms of employee productivity, product delays, Intellectual property losses, etc. in 2010?"

Participants' level of confidence in knowing when their company is being cyber attacked increased after the Test Bed. Across all categories (overall, decision makers, and non–decision makers), participants' level of confidence in knowing when their company is being attacked was higher after the Test Bed than before. As displayed in Table 19, participants' level of confidence increased by 11% after completing the Test Bed.

Table 19. Participants' Level of Confidence in Knowing When They Are Being Attacked

Category	All Participants		Decision Makers		Non–Decision Makers	
Interview	Pre	Post	Pre	Post	Pre	Post
Sample Size (n)	15	22	6	9	9	13
Average	39.1	50.1	55.0	58.3	28.4	44.4
Variance	9.3	9.8	11.0	10.5	6.3	9.3

This analysis refers to Question 26a in the Pre-Interview Guideand Question 18a in the Post-Interview Guide : "If greater than "Never," how confident are you that your company is aware when you're being attacked?"

The increase in the level of confidence from after the Test Bed may suggest that Test Bed staff provided knowledge and tools that made decision makers and non–decision makers feel better able to detect cyber security attacks.

Participants' perception of the likelihood that a cyber-criminal will attack increased after the Test Bed. Across all categories (overall, decision makers, and non–decision makers), participants' perception of the likelihood of a cyber-criminal attack was higher after the Test Bed experience than before. As displayed in Table 20, participants' view of the likelihood of a cyber-criminal attack increased from 46.9% before the Test Bed to 64.0% after.

Table 20. Participants' Perception of the Likelihood a Cyber Criminal Will Attack

Category	All Participants		Decision Makers		Non–decision Makers	
Interview	Pre	Post	Pre	Post	Pre	Post
Sample Size (n)	20	23	9	9	11	14
Average (dollars)	46.9	64.0	59.7	72.2	36.5	58.6
Variance	16.4	13.3	19.0	15.2	13.3	12.3

This analysis refers to Question 27 in the Pre-Interview Guide and Question 19 in the Post-Interview Guide : "On a scale from 0% to 100%, what is your perception of the likelihood that your company will be attacked by a cyber criminal (inside or outside the company) in the next year?"

The increase in the perception of the likelihood of cyber-criminal attack from before to after the Test Bed may suggest that information from the Test Bed has changed participants' views on the frequency of cyber attacks. Before completing the Test Bed, participants may have believed their company was too small to be targeted by a cyber-criminal. After the Test Bed experience, participants may now see their company as more likely to be the target of an attack by a cyber-criminal.

Participants' knowledge of solutions available for all potential security threats changed after the Test Bed. As Table 21 summarizes, the percentage of participants who felt they knew the solutions available for most threats increased from 15.8% before the Test Bed to 17.4% after. This increase was largely a result of the 31.9% jump in the number of decision makers who felt they knew the solutions available for most threats after completing the Test Bed. The percentage of non–decision makers who said they knew the solutions available for most threats fell from 18.2% before the Test Bed to 0% after.

The increase in the percentage of decision makers who indicated that they knew the solutions available for most threats may suggest that information presented in the Test Bed experience provided decision makers with a better understanding of available cyber security resources.

Participants' knowledge of where to find information about cyber security threats increased after the Test Bed experience. Across all categories (overall, decision makers, and non–decision makers), participants' knowledge of where to find cyber security threat information was higher after the Test Bed experience than before. As displayed in Table 22, 86.4% of participants said they knew where to go to get information about threats after the Test Bed, compared to 81.0% before. In addition, the percentage of decision makers who said they knew where to get information about threats jumped from 77.8% before the Test Bed to 100% after.

Table 21. Participants' Knowledge of Cyber Security Solutions

Category	Percent (%)					
	All Participants		Decision Makers		Non–Decision Makers	
Interview	Pre	Post	Pre	Post	Pre	Post
Sample Size (n)	19	23	8	9	11	14
I know what solutions are available for all threats	0.0	0.0	0.0	0.0	0.0	0.0
I know what solutions are available for most threats	15.8	17.4	12.5	44.4	18.2	0.0
I know what solutions are available for some threats	52.6	52.2	62.5	44.4	45.5	57.1
I know what solutions are available for a few threats	26.3	26.1	12.5	11.1	36.4	35.7
I do not know what solutions are available for any threats	5.3	4.3	12.5	0.0	0.0	7.1

This analysis refers to Question 28 in the Pre-Interview Guide and Question 20 in the Post-Interview Guide: "Which statement best describes your knowledge of potential solutions available for all potential security threats to your company?"

Table 22. Participants' Knowledge of Threat Information Location

Category	Percent (%)					
	All Participants		Decision Makers		Non–Decision Makers	
Interview	Pre	Post	Pre	Post	Pre	Post
Sample Size (n)	21	22	9	9	12	13
Yes	81.0	86.4	77.8	100.0	83.3	76.9
No	19.0	13.6	22.2	0.0	16.7	23.1

This analysis refers to Question 29 in the Pre-Interview Guideand Question 21 in the Post-Interview Guide: "Do you know where go to get information about threats?"

The increase in participants' knowledge of where to get threat information suggests that the Test Bed played a role in increasing decision makers' understanding of available cyber security resources. For example, decision makers may now know where to locate information for potential industry-specific cyber threats.

Participants' stated/perceived knowledge of where to find information on potential solutions increased after the Test Bed. Overall and within the decision maker category, participants' knowledge of where to find cyber security solution information was higher after the Test Bed than before. As displayed in Table 23, 87.0% of participants said that they knew where to go to get information about threats after the Test Bed, compared to 81.8% before. In addition, the percentage of decision makers who said they knew where to get information about solutions jumped from 58.3% before the Test Bed to 100% after.

Table 23. Participants' Knowledge of Solution Information Location

Category	Percent (%)					
	All Participants		Decision Makers		Non–Decision Makers	
Interview	Pre	Post	Pre	Post	Pre	Post
Sample Size (n)	21	23	9	9	12	14
Yes	81.8	87.0	58.3	100.0	83.3	78.6
No	19.0	13.0	22.2	0.0	16.7	21.4

This analysis refers to Question 30 in the Pre-Interview Guide and Question 22 in the Post-Interview Guide : "Do you know where to go for information on potential solutions?"

The average increase in stated/perceived knowledge of where to find cyber security solution information within the overall and decision maker category suggests that the Test Bed experience had a positive impact in increasing participants' understanding of available cyber security resources. Of note, however, is that non–decision makers indicated a slightly lower stated/perceived knowledge of information on cyber security solutions after the Test Bed as opposed to before (83.3% before versus 78.6% after). This may be because the Test Bed experience provided a significant amount of information about cyber security solutions, which likely increased Test Bed participants' knowledge but may have decreased their perceived knowledge (they may have thought they knew more than they actually did before the Test Bed experience). In the case of decision makers, who are more comfortable with cyber security terminology, it is possible that the increase can be interpreted simply as an increase in knowledge based on the Test Bed experience.

Participants' responses on who they ask for cyber security advice changed somewhat after the Test Bed. As seen in Table 24, participants were most likely to seek advice from an IT professional or a vendor who they bought software or hardware from both before and after the Test Bed. The percentage of participants who asked a friend for cyber security advice jumped from 4.3% before the Test Bed to 30.4% after.

Some changes were seen in the cyber security knowledge of participants after the Test Bed. Responses from participants indicated a higher percent change of experiencing a cyber security attack after the Test Bed; however, responses from participants also indicated an increase in the confidence that their companies would be able to detect a cyber-attack after completing the Test Bed. In addition, a higher percentage of decision-makers indicated that they knew the solutions available for most cyber security threats and they knew where to look for cyber security threat and solution information.

Table 24. Resources for Cyber Security Advice

Category	Percent (%)					
	All Participants		Decision Makers		Non–Decision Makers	
Interview	Pre	Post	Pre	Post	Pre	Post
Sample Size (n)	23	23	9	9	14	14
IT professional (support service)	82.6	91.3	77.8	77.8	85.7	100.0
Vendor who you bought software/hardware from	26.1	47.8	11.1	44.4	35.7	50.0
Your Internet service provider (ISP)	13.0	21.7	11.1	22.2	14.3	21.4
A friend	4.3	30.4	0.0	11.1	7.1	42.9
A family member	4.3	17.4	0.0	11.1	7.1	21.4
Other	17.4	30.4	22.2	44.4	14.3	21.4

This analysis refers to Question 31 in the Pre-Interview Guide and Question 23 in the Post-Interview Guide: "Who do you ask for cyber security advice?"

4.4 Cyber Security Information Needs

The following section discusses participants' qualitative responses to questions regarding the barriers to adoption of appropriate IT security technologies, the availability of adequate information to make security decisions, and the factors that would motivate participants to spend more on cyber security.

Participants' responses regarding the barriers to adoption of appropriate IT security technologies within their industry were similar among companies. Convenience and cost were cited as the most common barriers to the adoption of appropriate IT security technologies. One participant explained the importance of convenience by noting that individuals often want to access their computers without going through a bunch of hurdles. In explaining cost as a barrier, another participant noted that the cost-benefit analysis often does not make it worthwhile to invest in cyber security. Additional barriers mentioned by participants included a lack of awareness and appreciation of cyber threats, and a lack of full-time staff available to monitor cyber security issues.

Participants' responses regarding whether their company had all of the necessary information to make the best decision on IT security solutions were mixed. Many participants said they knew more information now than before the Test Bed, but they did not think they necessarily had all the information. Participants' suggestions for additional information included increased awareness of cyber security issues, regularly updated information on cyber threats, and websites containing cyber security best practices.

Participants overwhelmingly cited a major security breach or cyber attack as the primary factor that would incentivize them to spend more on cyber security. The response from one participant provided some insight on why an attack was the most frequent incentive. The participant explained: "People are generally not proactive because they think that they don't have anything [the attackers] want. This is why the awareness thing is important; there is a general lack of understanding of what's going on." Although

most of the incentives to spend on cyber security relied on a reactive approach, several participants said that having additional information would incentivize them to spend more on cyber security. For example, participants from one company thought receiving information on how specific cyber attacks have hurt other businesses in their industry would be helpful in making cyber security spending decisions. Another participant noted that an analysis of the impact of the threat on his business would be especially helpful because he did not know whether some of the threats were meaningful. Lastly, several participants also indicated that additional funding, such as grants from the government, would allow them to spend more on cyber security.

Not surprisingly, time, money, and convenience were cited most commonly by participants as the primary barriers to the adoption of appropriate cyber security technologies. Many participants noted that they did not have all the information necessary to make cyber security decisions, and some pointed out that they could use regularly updated information on cyber threats and access to websites containing cyber security best practices. Lastly, an overwhelming number of participants cited a major security breach or cyber attack as the primary factor that would incentivize them to spend more on cyber security.

4.5 The Cyber Test Bed Experience

The following section summarizes participants' responses to questions about the Cyber Test Bed experience. The section includes feedback from participants on the overall Test Bed experience, the usefulness of certain Test Bed items, and the amount of resources (time and money) participants invested during and after the Test Bed. The section also includes estimates from participants on the amount of money they would be willing to pay for the Test Bed and whether participants made or plan to make changes recommended by Cyber Test Bed staff.

Responses from after the Test Bed indicate that participants found it to be very valuable. As summarized in Table 25, the Test Bed received an average rating of 8 from participants on a scale of 1 to 10 where 1 indicates the experience was not very valuable and 10 indicates the experience was highly valuable. Although both decision makers and non–decision makers placed a high value on the Test Bed, the average rating of the Test Bed experience among decision makers (9) was slightly higher than the average rating among non–decision makers (7.3). Responses from decision makers ranged from 6 to 10 and responses from non–decision makers ranged from 3 to 10.

Table 25. Value Placed on the Test Bed

Category	All Participants	Decision Makers	Non–Decision Makers
Sample Size (n)	22	9	13
Average	8.0	9.0	7.3
Variance	4.7	3.0	4.9

The analysis is based on Question 24 in the Post-Test Bed Interview Guide: "How valuable was the Cyber TB experience?" (1= the experience was not very valuable, 10 = the experience was highly valuable).

The high overall average response ratings indicate that participants found the Test Bed experience to be highly valuable. The slight difference in ratings between decision makers and non–decision makers

may be because decision makers found the Test Bed experience to be more relevant to their position in the company than non–decision makers. For instance, participants who indicated that they are not involved in the cyber security decision making process at their company may have felt that pieces of the Test Bed were not particularly valuable or relevant to their position. Still, the average value participants placed on the Test Bed experience was high among all categories, suggesting that the Test Bed was helpful to participating companies.

Participants found certain aspects of the Test Bed to be more valuable than others. Table 26 and Figure 2 summarize the ratings participants placed on the value of Test Bed–related items. A lower number in this case indicates that a higher value was placed on the Test Bed item. Participants did not need to rank all of the items, and were able to rank more than one item the same. The sample size for each component is noted in Table 26. Test Bed items with the highest average ranking included the first threat briefing (2.2), the first asset protection session (2.6), and the second threat briefing (2.7). The three newsletters received the lowest average rankings among the Test Bed activities. The responses between decision makers and non–decision makers do not differ greatly, although decision makers placed a slightly higher average value on the newsletters than non–decision makers (possibly because they were more interested in both the brevity and the level of detail—which did require some cyber security knowledge—that they provided on cyber security threats and potential solutions, than were non–decision makers).

Of note, portions of the Test Bed were customized for each company, and as such, the actual experiences in each of these Test Bed components may have been slightly different. The newsletters were the same for all companies, but otherwise, information provided may have been slightly different—either because it was tailored to the company or because questions posed and answered by a specific company were likely different in each instance.

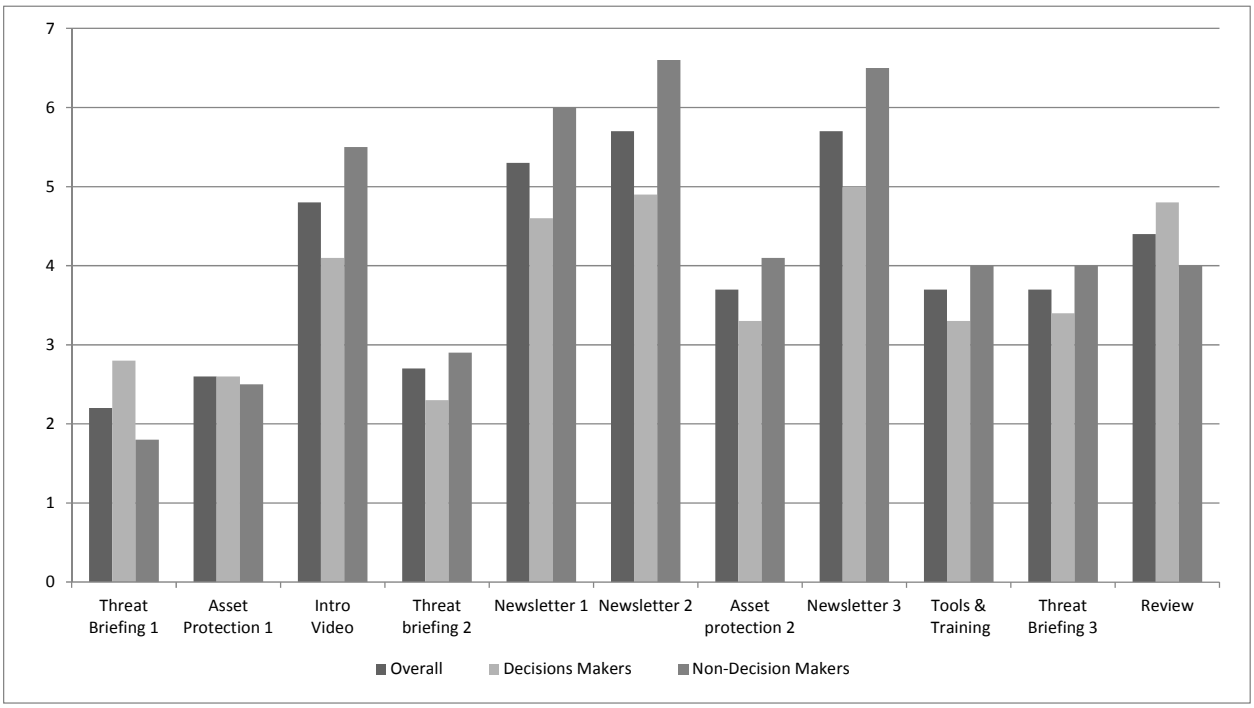
Given that no Test Bed component was rated as higher than 6.6 out of 11 (where 11 indicated that something was a “least valuable” component of their cyber security strategy), these data suggest that in general companies were satisfied with all components of the Cyber Test Bed experience.

Table 26. Average Value of Test Bed Components

Category	All Participants		Decision Makers		Non–Decision Makers	
	n	Rating	n	Rating	n	Rating
Threat Briefing 1	23	2.2	9	2.8	14	1.8
Asset Protection 1	20	2.6	9	2.6	11	2.5
Intro Video	13	4.8	7	4.1	6	5.5
Threat briefing 2	22	2.7	9	2.3	13	2.9
Newsletter 1	15	5.3	7	4.6	8	6
Newsletter 2	14	5.7	7	4.9	7	6.6
Asset protection 2	19	3.7	9	3.3	10	4.1
Newsletter 3	13	5.7	7	5	8	6.5
Tools & Training	18	3.7	9	3.3	9	4
Threat Briefing 3	18	3.7	9	3.4	9	4
Review	15	4.4	8	4.8	7	4

The analysis is based on Question 25 in the Post-Test Bed Interview Guide: "Which pieces were most valuable in terms of the effect on your organization's cyber security strategy?" (1=most valuable, 11=least valuable).

Figure 6. Average Rank of Test Bed Components



The analysis is based on the following sample sizes: All Participants=23, Decision Makers=9, Non–decision Makers=14.

Tables 27 and 28 summarize the average amount of time participants invested in the Test Bed and the average amount of time companies invested in the Test Bed. On average, individual participants invested 22.1 hours in the Test Bed. Decision makers invested an average of 27.6 hours in the Test Bed, while non–decision makers invested an average of 18.6 hours. Companies invested 118.7 hours in the Test Bed. Interestingly, decision makers indicated that their companies invested an average of 15 hours less in the Test Bed than non–decision makers. Given that decision makers likely have more accurate information on time spent on cyber security across an organization, non–decision makers are probably overestimating the investment.

Table 27. Amount of Time Interview Participants Invested in the Test Bed

Category	All Participants	Decision Makers	Non–Decision Makers
Sample Size (n)	23	9	14
Average (hours)	22.1	27.6	18.6
Variance (hours)	421.2	793.0	191.0

The analysis is based on Question 26 in the Post-Test Bed Interview: "How much time did you invest in the Cyber TB experience?"

Table 28. Amount of Time Companies Invested in the Test Bed

Category	All Participants	Decision Makers	Non–Decision Makers
Sample Size (n)	16	9	7
Average (hours)	118.7	112.1	127.1
Variance (hours)	6,480.4	5,196.6	9,123.8

The analysis is based on Question 26 in the Post-Test Bed Interview Guide: "How much time did your company invest in the Cyber TB experience?"

Table 29 summarizes the average amount of capital and labor participants estimated their companies invested during the Test Bed as a result of the Test Bed experience, and Table 30 summarizes the average amount of capital and labor participants estimated their companies invested after the Test Bed as a result of the Test Bed experience. On average, participants estimated their companies invested an average of $4,942.90 during the Test Bed. Decision makers estimated that an average of $4,616.70 was invested during the Test Bed, while non–decision makers estimated that $5,187.50 was invested. Again, decision makers likely have the ability to estimate this more accurately than do non–decision makers based on their role in the organization.

Table 29. Amount of Money Invested in Cyber Security During the Test Bed

Category	All Participants	Decision Makers	Non–Decision Makers
Sample Size (n)	14	6	8
Average	$4,942.90	$4,616.70	$5,187.50
Variance	67,422,637.4	25,681,666.7	106,709,821.4

The analysis is based on Question 27a in the Post-Test Bed Interview Guide: "How much money (if any) did you invest during the Cyber TB experience (as a result of the Cyber TB experience)?"

Table 30. Amount of Money Invested in Cyber Security After the Test Bed

Category	All Participants	Decision Makers	Non–Decision Makers
Sample Size (n)	15	7	8
Average	$1,466.70	$2,857.10	$250.00
Variance	26,552,381.0	57,142,857.1	500,000.0

The analysis is based on Question 27b in the Post-Test Bed Interview Guide: "How much money (if any) did you invest after the Cyber TB experience (as a result of the Cyber TB experience)?"

On average, participants indicated that companies invested $1,466.70 after the Test Bed. Decision makers estimated that an average of $2,857.10 was invested after the Test Bed, while non–decision makers estimated that $250 was invested after. It is important to note that participants were interviewed shortly after the completion of the Test Bed, and some participants pointed out that they had not yet invested in cyber security but planned to do so in the future.

Table 31 summarizes participants' willingness to pay (as a "yes" or "no") for the Test Bed experience, and Table 32 summarizes the average amount of money participants would be willing to pay for the Test Bed. The majority of participants (77.3%) indicated that they would be willing to pay for the Test Bed. The percentage of participants who indicated a willingness to pay for the Test Bed was slightly higher among decision makers (88.9%) than non–decision makers (69.2%).

Table 31. Participants' Willingness to Pay for the Test Bed (Post-Test Bed)

Category	Percent (%)		
	All Participants	Decision Makers	Non–Decision Makers
Sample Size (n)	22	9	13
Yes	77.3	88.9	69.2
No	22.7	11.1	30.8

The analysis is based on Question 28 in the Post-Test Bed Interview Guide: "Understanding the value of the Cyber TB to companies such as yours helps the government determine what role it should play in cyber security. Knowing what you know now, prior to your participation, if the Cyber Test Bed were offered to you as a service for a price, would you be willing to pay for it?"

Table 32. Amount of Money Participants Were Willing to Pay for the Cyber Test Bed Experience (Post-Test Bed)

Category	Dollars ($)		
	All Participants	Decision Makers	Non–Decision Makers
Sample Size (n)	16	8	8
Average	7,881.3	7,075.0	8,687.5

The analysis is based on Question 28a in the Post-Test Bed Interview Guide: "If Yes, how much would you have been willing to pay?"

On average, participants said they would be willing to pay $7,881.30 for the Test Bed experience. This average does not include individuals who indicated that they would not be willing to pay anything for the Test Bed. Of the individuals willing to pay for the Test Bed, responses ranged from $600 to $25,000. These results suggest that providing a Test Bed experience with its most popular components would be something that small and mid-size businesses would likely be willing to pay for. The results also suggest that current cyber security training service offerings may not be of sufficient quality to meet demand or may be too expensive for small and mid-size businesses.

Table 33 summarizes the amount of money participants are willing to pay for the Test Bed after having completed it. The responses indicate that the amount of money participants are willing to spend after completing the Test Bed is approximately 60% higher than what they would have been willing to spend prior to participating in the Test Bed. Participants willing to spend a higher amount on the Test Bed indicated that they would spend $5,888 more than they would have been willing to spend prior to participating in the Test Bed.

Table 33. Change in Amount of Money Participants Are Willing to Pay After the Test Bed

Category	All Participants	Decision Makers	Non–Decision Makers
Sample Size (n)	20	8	12
Higher	60.0%	62.5%	58.3%
Not higher	40.0%	37.5%	41.7%
How much higher	$5,888	$6,400	$5,595

The analysis is based on Question 28b in the Post-Test Bed Interview Guide: "Is this amount higher than you would have been willing to pay prior to participation? If so, how much higher?"

This finding suggests that there may be significant difficulty convincing small and mid-size businesses to pay for cyber security training services. Without adequate knowledge of the value of the experience, many small and mid-size businesses may be hesitant to pay for such services.

Companies that participated in the Test Bed program adopted the changes recommended by the Cyber IT staff. As seen in Table 34, a majority of participants (90.5%) indicated that their companies made changes recommended by the Test Bed staff. Documenting policies, improving physical security, using separate computers for financial transactions, and updating virus and network intrusion protection software were among some of the changes participants cited in their responses. The percentage of decision makers who indicated that they had made changes recommended by the Test Bed staff was 16.7% higher than the percentage of non–decision makers. Decision makers may have been more likely than non–decision makers to be involved in implementing cyber security–related changes at their company, perhaps explaining the differences in responses between the two categories.

Table 34. Implementation of Changes Recommended by Test Bed Staff

Category	Percent (%)		
	All Participants	Decision Makers	Non–Decision Makers
Sample Size (n)	21	9	12
Yes	90.5	100.0	83.3
No	9.5	0.0	16.7

The analysis is based on Question 29 in the Post-Test Bed Interview Guide: "Have you made changes recommended by the Cyber TB staff?"

A majority of participants (88.2%) indicated that they plan to make changes recommended by the Test Bed staff, as summarized in Table 35. These responses were very similar to the previous responses discussing the recommended changes that companies had already implemented. In a few of the responses, participants mentioned plans to continue implementing and documenting cyber security policies and improving their employee training programs. One participant also noted that after undergoing the Test Bed, his company planned to incorporate cyber security into the next year's strategic plan.

Table 35. Future Implementation of Changes Recommended by Test Bed Staff

Category	Percent (%)		
	All Participants	Decision Makers	Non–Decision Makers
Sample Size (n)	17	8	9
Yes	88.2	100.0	77.8
No	11.8	0.0	22.2

The analysis is based on Question 30 in the Post-Test Bed Interview Guide: "Do you plan to make changes recommended by the Cyber TB staff?"

A majority of participants (72.2%) said that they did not make changes that differed from what the Test Bed staff recommended, as summarized in Table 36. However, contrary to the Test Bed staff's recommendations, two participants noted that they continued to allow remote network access and use Dropbox for convenience purposes. A third participant noted that he was not able to successfully implement one piece of software recommended by the Test Bed staff, and he is currently looking for an alternative option.

Table 36. Changes Made That Were Not Recommended by Test Bed Staff

Category	Percent (%)		
	All Participants	Decision Makers	Non–Decision Makers
Sample Size (n)	18	8	10
Yes	27.8	25.0	30.0
No	72.2	75.0	70.0

The analysis is based on Question 31 in the Post-Test Bed Interview Guide: "Are there areas where you made changes that differ from what the Cyber TB staff recommended?"

As seen in Table 37, a majority of participants (58.8%) indicated that their company planned to increase cyber security spending by an average of 20.6%. An even higher majority of decision makers (71.4%) planned to increase cyber security spending in the future. Given that decision makers are likely to have accurate knowledge of company spending priorities, it seems that cyber security spending will be an important factor in future budgets. However, because this question was not asked before the Test Bed, it is unclear whether or how the amount of money participants planned to spend changed after the Test Bed.

Table 37. Companies' Plans for Future Spending in Cyber Security

Category	Percent (%)		
	All Participants	Decision Makers	Non–Decision Makers
Sample Size (n)	17	7	10
Increase	58.8	71.4	50.0
Decrease	0.0	0.0	0.0
Stay the same	35.3	28.6	40.0
Average % increase among those who chose "Increase"	20.6	22.3	17.3

The analysis is based on Question 32 in the Post-Test Bed Interview Guide: "Do you plan to increase, decrease, or not change your spending on cyber security?"

Table 38 summarizes the Test Bed companies' plans to record IT security resources before and after the Test Bed. In all seven response options, the percentage of overall participants and decision makers planning to record IT security resources increased after the Test Bed experience. For example, the percentage of participants planning to record the resources spent gathering information (e.g., from CERTs, SANS, Gartner) increased from 8.3% before the Test Bed to 25.0% after. The percentage of non–decision makers planning to record IT security resources increased in all but one of the categories. Recording resources spent on testing IT security measures dropped from 25.0% before the Test Bed to 18.2% after.

Table 38. Companies' Plans to Record IT Security Resources

Category	All Participants (%)		Decision Makers (%)		Non–Decision Makers (%)	
Interview	Pre	Post	Pre	Post	Pre	Post
Sample Size (n)	20	20	9	9	11	11
Installing new IT security measures	25.0	35.0	25.0	44.4	25.0	27.3
IT security staff education	16.7	25.0	16.7	33.3	16.7	18.2
Gathering information (e.g., from CERTs, SANS, Gartner)	8.3	25.0	8.3	33.3	8.3	18.2

Testing IT security measures	16.7	25.0	8.3	33.3	25.0	18.2
Monitoring IT security status	20.8	25.0	25.0	33.3	16.7	18.2
Responding to IT security problems	29.2	35.0	33.3	44.4	25.0	27.3
Other	8.3	15.0	8.3	22.2	8.3	9.1

The analysis is based on Question 35 in the Pre-Test Bed Interview Guide and Question 33 in the Post-Test Bed Interview Guide: "Do you plan to record your IT security resources (e.g., the number of hours spent by IT staff) allocated toward the following specific activities?"

The increase in the percentage of participants indicating that their companies plan to record IT security resources suggests that information from the Test Bed may have encouraged companies to better track the amount of time and money spent on IT security. The decrease in the percentage of non–decision makers planning to record IT security resources may be a result of financial constraints in Test Bed companies. Recording the resources spent on testing IT security measures would increase the work burden on non–decision makers or would require hiring additional staff. Additionally, non–decision makers may have seen this as a highly technical area and not within their area of specialty or ability.

The number of cyber security training hours participants said IT staff would receive each year changed after the Test Bed. Figures 3, 4, and 5 summarize the amount of cyber security training participants said IT staff would receive each year. The percentage of participants indicating that IT staff would receive 15–19 hours per year and 20+ hours per year increased after the Test Bed while the percentage of participants indicating that staff would receive 14 hours per year or less decreased after the Test Bed.

Figure 7. Amount of Cyber Security Training for IT Staff each Year (All participants, n=14 pre/15 post)

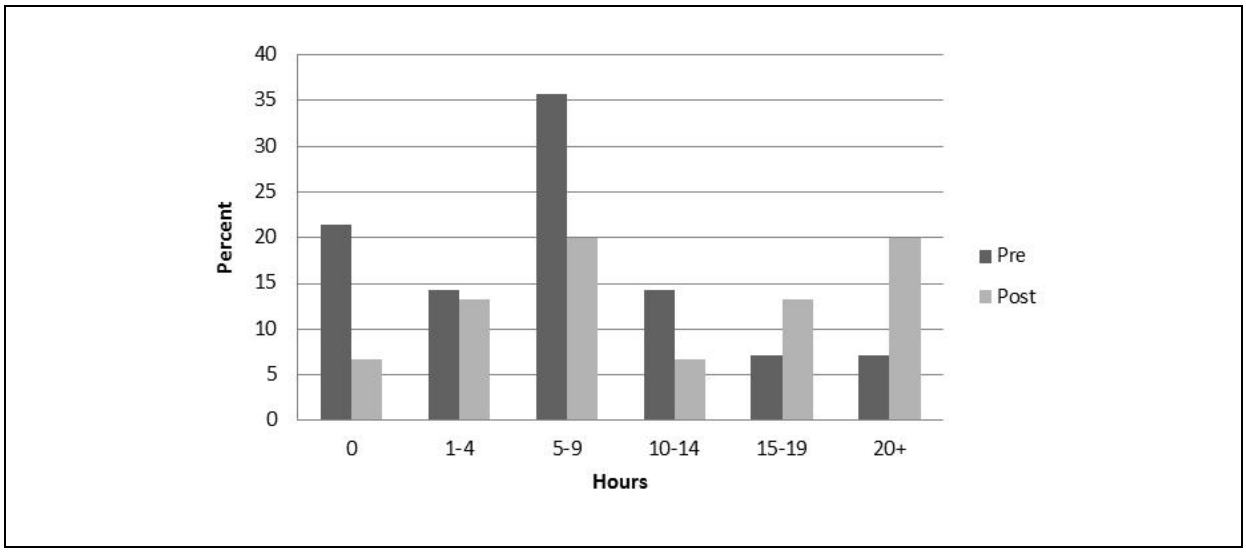


Figure 8. Amount of Cyber Security Training for IT Staff each Year (Decision Makers, n= 7 pre/ 9 post)

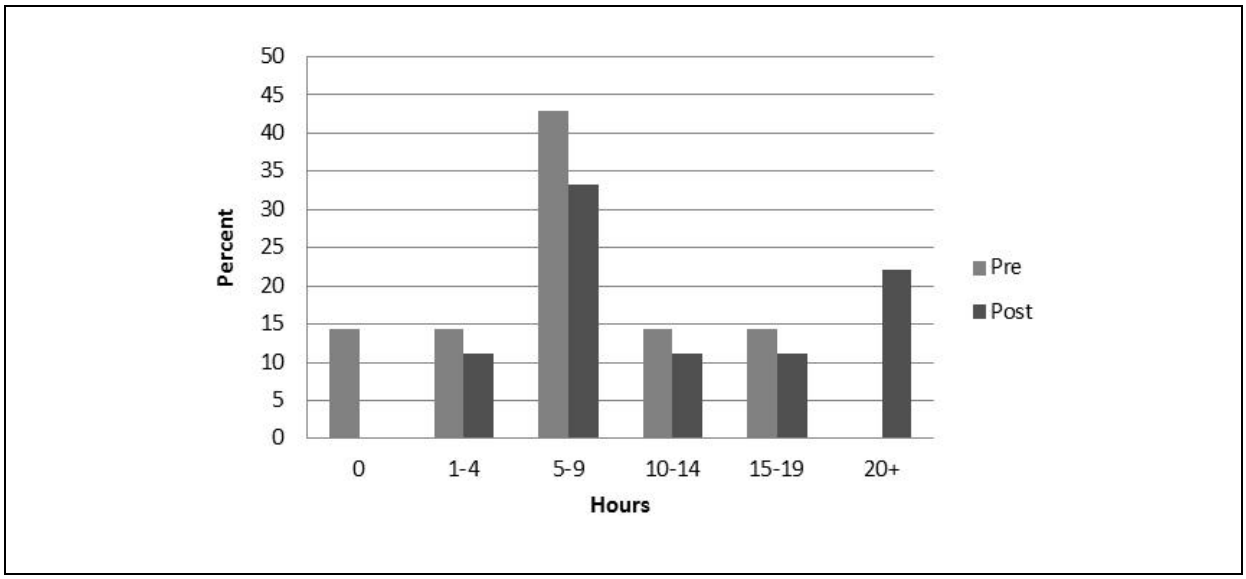
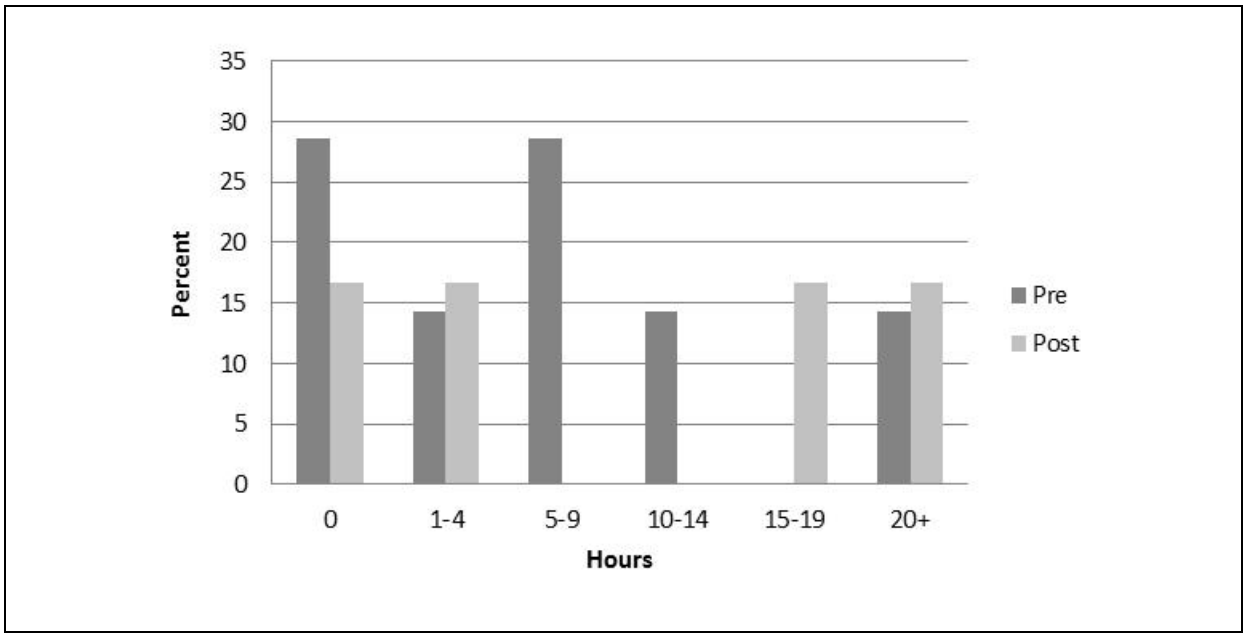


Figure 9. Amount of Cyber Security Training for IT Staff (Non–Decision Makers, n= 7 pre/ 6 post)



The analysis in Figures 3, 4, and 5 is based on Question 36 in the Pre-Test Bed Interview Guide and Question 34 in the Post-Test Bed Interview Guide: "How much training will your IT staff receive each year on new cyber security technologies and threats?"

The increase in the number of the hours per year IT staff will receive at companies that participated in the Test Bed suggests that information from the Test Bed may have heightened the priority for annual cyber security training.

The number of cyber security training hours participants said regular staff would receive each year changed after the Test Bed. Figures 6, 7, and 8 summarize the amount of cyber security training participants indicated that regular staff would receive each year. The percentage of participants indicating that regular staff would receive 1 hour or more of cyber security training each year increased after the Test Bed. The percentage of participants who said regular staff would receive 1–2 hours per year of cyber security training, for example, jumped from 38.9% before the Test Bed to 66.7% after.

The increase in the number of hours per year regular staff will receive at companies that participated in the Test Bed suggests that information from the Test Bed may have heightened the priority for annual cyber security training.

Participants' responses indicated an increased awareness of the methods available to enforce cyber security policies at their companies. As seen in Table 39, 25% of participants said they did not know how their company planned to enforce cyber security policies before the Test Bed. Participants often said they were unaware of any formal mechanisms to enforce cyber security policies. However, after completing the Test Bed, a larger number of participants reported the use of manual and automated tools to enforce cyber security policies. This change in cyber security enforcement is evident in some of the explanations from participants. For example, before the Test Bed, one participant said that he did not know of any ways his company enforced cyber security policies. After the Test Bed, the same participant explained that his company monitors cyber security policies by "checking up on [the employees] (we only have 30 people) and sending out reminder e-mails."

Figure 10. Amount of Cyber Security Training for Regular Staff (All participants, n=18)

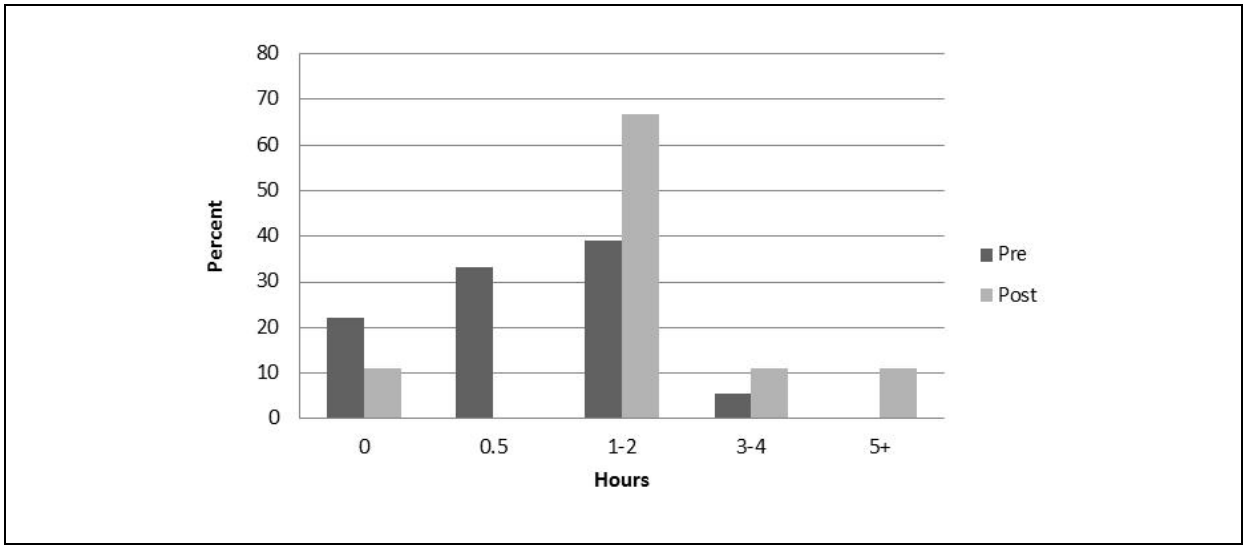


Figure 11. Amount of Cyber Security Training for Regular Staff (Decision Makers, n=9)

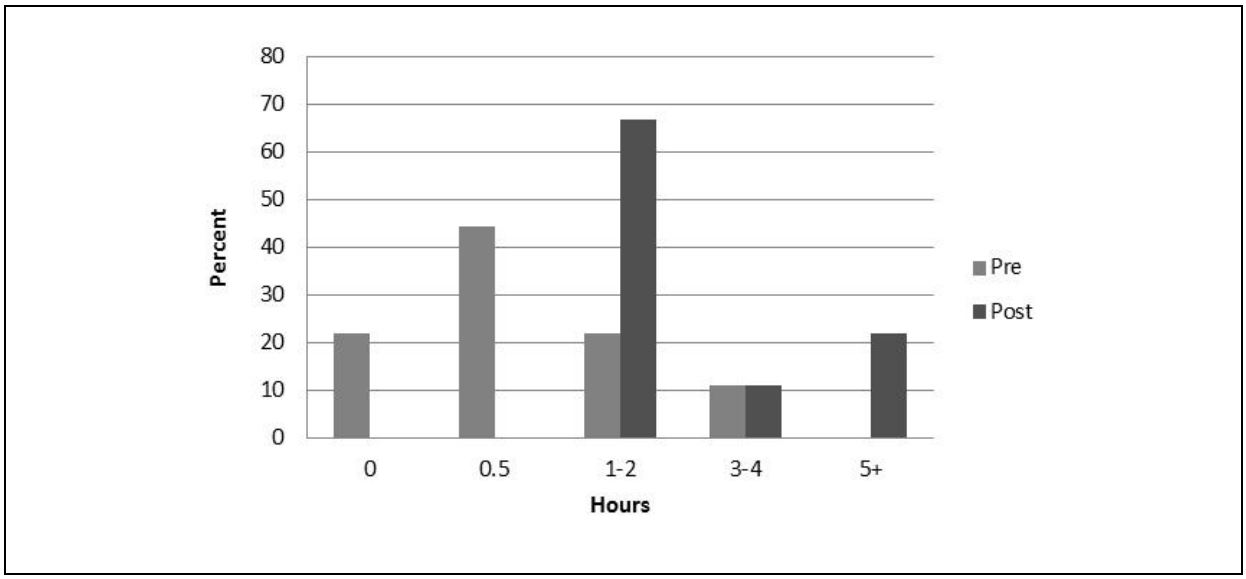
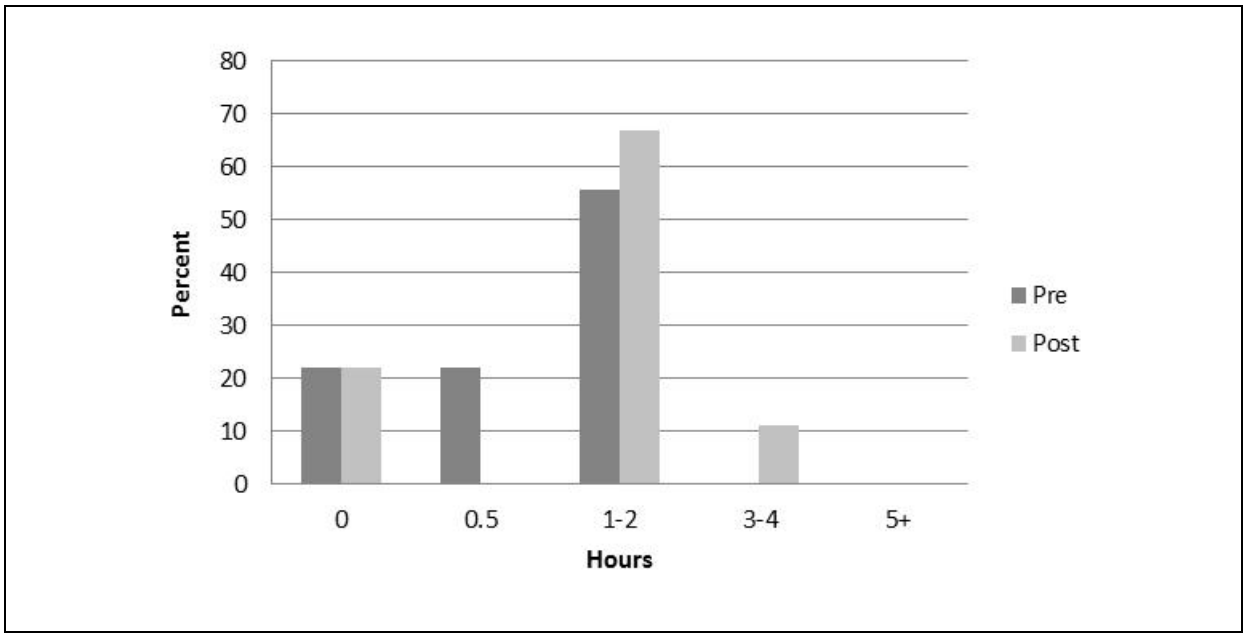


Figure 12. Amount of Cyber Security Training for Regular Staff (Non–Decision Makers, n=9)



The analysis for Figures 6, 7, and 8 is based on Question 37 in the Pre-Test Bed Interview Guide and Question 35 in the Post-Test Bed Interview Guide: "How much training will your regular staff receive on cyber security threats/policies?"

Table 39. Companies' Plans to Monitor/Enforce Cyber Security Policies

Category	Percent (%)					
	All Participants		Decision Makers		Non–Decision Makers	
Interview	Pre	Post	Pre	Post	Pre	Post
Sample Size (n)	20	15	8	7	12	8
Manually	35.0	40.0	62.5	14.3	16.7	62.5
Automated tools	30.0	20.0	12.5	42.9	41.7	0.0
Both	10.0	26.7	25.0	42.9	0.0	12.5
Don't Know	25.0	0.0	0.0	0.0	41.7	0.0
Neither	0.0	13.3	0.0	0.0	0.0	25.0

The analysis is based on Question 39 in the Pre-Test Bed Interview Guide and Question 37 in the Post-Test Bed Interview Guide: "How do you plan to monitor/enforce staff compliance with cyber security policies?"

Interestingly, the percentage of decision makers who planned to enforce cyber security with automated tools increased from 12.5% to 42.9% after the Test Bed. A greater percentage of non–decision makers, on the other hand, planned to enforce cyber security policies manually (16.7% to 62.5%). The difference in cyber security policy enforcement strategies between decision makers and non–decision makers highlights a difference in perspective among the two groups. Decision makers may aim to use manual tools in the future, while non–decision makers may feel that manual enforcement is more likely at their small business.

Feedback from participants regarding the Cyber Test Bed was generally positive. Most participants found the Test Bed to be very valuable and found the threat briefing and asset protection pieces of the Test Bed to be particularly useful. Participants estimated that they invested an average of 22.1 hours in the Test Bed and their company invested an average of 118.7 hours in the experience. Participants estimated that their companies invested an average of $4,942.90 during the Test Bed. After completing the Test Bed, a majority of participants said they would be willing to spend an average of $7,881 for it. Most participants stated that they implemented or planned to implement changes recommended by the Test Bed staff. A majority of decision makers also indicated that they planned to increase spending on cyber security in the future.

4.6 Qualitative Feedback Received During Interviews

The following section discusses participants' feedback to questions about the Cyber Test Bed experience. The section includes a summary of participant responses to questions regarding surprising information learned during the Test Bed, whether companies reprioritized their or their IT objectives, whether the Test Bed would be useful to other companies, and whether the federal government should be involved in funding cyber security at companies.

A majority of participants in the Test Bed (19) indicated that they were surprised by some of the things they learned during the project. Most commonly, participants said they were surprised by the number and the extent of the threats that existed. For example, one participant explained that he was

surprised by "the prevalence of threats and how it's happening local, like right down the street where we do business and our companies live. I knew this, but this experience made it real—not just theoretical." Participants were also surprised by the number of potential foreign threats against their company's cyber security. Several participants, for example, said the Test Bed staff helped them identify foreign malware that had been embedded in external devices. Lastly, a few participants were surprised by some of the financial security information provided by Test Bed staff. These participants said they were previously unaware that business and consumer banking accounts did not have the same level of protections.

Participants' responses regarding whether they reprioritized any of their company objectives based on the Test Bed experience were mixed. Most of the participants who responded to this question said they did not reprioritize any of their company objectives. A few participants did mention that after the Test Bed experience, their company heightened the priority of cyber security. Although most participants did not make changes to company priorities after the Test Bed, one participant did share this response: "We overhauled our whole security broker to make sure they have the correct security standards. We usually rush to get new features to market at the expense of security, so now before we roll stuff out we make sure encryption certificates and everything is set up. Security breaches result in a loss of customer confidence, which then leads to loss in revenue, so that's what makes us do what we do."[10]

More participants indicated that they reprioritized their IT security objectives than company objectives based on the Test Bed experience. In addition to increasing the priority placed on cyber security, participants also mentioned improving network management, monitoring IP theft from inside the company, and ensuring the presence of a working network IDS/IPS.

All but one of the participants thought that other companies would benefit from the Test Bed. Participants thought all companies, particularly those that deal with online financial transactions or are in the high-tech industry, would benefit the most from the Test Bed. Some participants also thought small to mid-size companies that lacked a large budget for IT resources would benefit from the Test Bed. The one participant who felt that other companies would not benefit from the Test Bed said that the information he received during the Test Bed was not easy to distribute and explain to other individuals. He suggested that the Test Bed provide "information to emphasize that [cyber security] is something we need to worry about, and then suggest three to four things to do."

Participants' responses were mixed regarding whether government should pay to support the cyber security of companies or private companies should pay on their own risk tolerance. Approximately half of the participants thought that private companies should be responsible for their own cyber security. The participants explained that cyber security is part of the cost of doing business, so private companies should pay based on their own risk tolerance. One participant explained, "private companies should pay [for cyber security] based on their own risk tolerance, because it's something that if you make a financial commitment to do, you will see it through and make the commitment." On the other hand, approximately one-third of participants felt that both government and private companies should pay to support cyber security. Several participants, for example, thought the government should be involved in matters of

[10] Note that this is only one respondent, and may not represent the views of other participants at the same company or participants at other companies.

national security. One participant explained, “private companies should pay for their own security, but the government should pay to prevent foreign threats if they are coming from one specific country…” Many of the participants who thought a combination of private sector and government support was necessary for cyber security noted that they were unsure of where to draw the line between the two.

Most participants indicated that they were surprised by some of the information they learned during the Test Bed, particularly about the number and extent of the cyber security threats that exist. Although not many participants indicated that they reprioritized their company objectives after the Test Bed, some participants did. Lastly, a majority of participants stated that other companies, particularly those that deal with online financial transactions and those in the high-tech industry, would benefit from the Test Bed.

4.7 Additional Qualitative Feedback Received and Observations Made During the Test Bed Experience

Throughout the Test Bed implementation, all but one company appeared to be completely engaged. All individuals interacted during our sessions in each stage. Despite our intention to be sensitive to each participant’s time contribution by keeping engagements under an hour, we were consistently asked to remain longer to help answer deeper questions and to help participants better understand each facet of security we covered.

In the case of the company that appeared to be resistant, the Test Bed team learned that most of its behavior was related to internal issues the company faced. Because the company was a partnership, most of its IT assets were personally owned and dual use devices. Senior partners grappled with how to institute policy changes they did not feel they were empowered to make. This company also had a difficult time trying to identify the root cause of its security issues. IT felt they were not empowered to make security changes either and assessed that many of the vulnerabilities found during our network scans were because they could not enforce security standards they felt needed to be applied. Partners were generally resistant to anything they perceived might impact their productivity. We devoted a number of extra hours to this company to help it through its unique challenges. Ultimately, it assigned risk management duties to one of the senior partners who was responsible for resolving network security shortfalls and implementing security policies.

Anecdotally, participants felt that the program was very informative. However, managers did not fully understand the importance of the training interactions until they received the results from their network vulnerability assessments. It became clear that the foundational training they received was critical to them understanding the information in the vulnerability assessment and helped them react and make decisions without fear. Simply providing a network vulnerability assessment without providing basic threat knowledge first would have either been viewed as a “scare tactic” or would not have been acted on simply because they would not have known how to accurately interpret the information.

Overall, the Test Bed operational team observed changes in attitudes and behaviors toward security and technical behaviors. For example, after the Test Bed experience, all participants indicated that they had already begun to include or were considering security in all facets of business and strategic

planning. They began to use or investigate the use of the provided policies and generally felt that the policy templates provided a great foundational framework to bring structure to cyber security efforts. Company executives also felt that they had a better understanding of their security needs, which translated into requirements made of specific staff. In particular, the Test Bed team received a great deal of positive feedback concerning the asset cards we developed and disseminated, which were designed as a quick reference and to stimulate discussions and questions about security.

Broadly, the following behavior changes were observed throughout the course of the project:

- Approximately one-third were in the process of implementing a recurring security awareness program (Lavender, Phlox, Coral)
- Over three-quarters (7 of 9) made changes (increased or added responsibilities) to staff to address security requirements (Phlox, Curacao, Honeysuckle, Coral, Silver, Lavender, Beeswax)
- One-third reserved computers strictly for travel that did not have corporate information or access (Curacao, Silver, Lavender)
- Two companies decided to completely rearchitect their network to address security concerns identified through the Test Bed project (Honeysuckle, Curacao)
- Two companies began integrating risk and security elements into operational and strategic business management decision making (Peony, Beeswax)
- One-third immediately made changes (security controls and limits) in how they conducted financial transactions (Silver, Curacao, Peony)
- One company implemented enterprise-wide encryption of data at rest, eliminated remote log-in and remote desktop capabilities, updated policies to incorporate security changes, and implemented a continuity of operations plan (Lavender)

5. Conclusions and Recommendations

Given the undesirable state of cyber security at most small and mid-size businesses, the Cyber Test Bed project was initiated to conduct a case study analysis of how a set of “interventions” including threat analysis, best practices sharing, and executive and staff training events would impact a group of fewer than 10 small and mid-size businesses. The project team worked with several external experts in cyber security to develop a robust set of tools and training exercises, and provided these to participating companies over approximately a 12-month period. The culmination of the experience was a summit in which participating companies and other companies were provided information on the Test Bed components and heard from several distinguished speakers from DHS and Congress.

Interviews were conducted both before and after the Test Bed experience, and additional qualitative information was collected by Cyber Test Bed staff during the Test Bed experience. Twenty-three individuals (at least two at each of the nine companies) participated in both sets of interviews; of these, 14 were self-labeled cyber security decision makers at their companies, and 9 were self-labeled

non–decision makers. Additionally, qualitative information was collected based on how companies reacted to Test Bed components in real time.

Both anecdotal evidence and interview results suggest that the majority of participants in the Cyber Test Bed perceived benefits from the experience. The interview data suggest that companies perceived a variety of benefits from many of the components of the Test Bed and that most participants (77.3%) would have been willing to pay for the experience. Overall, of those willing to pay more than $0 (16 participants), the average willingness to pay was $7,881.30. If priced appropriately, these sixteen companies would have participated, if they had known what the experience would be like. This is an important finding because it suggests that small and mid-size businesses are willing to pay for cyber security training, but they have not identified cyber security training that they believe to be worth their money. This could mean several things:

- 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.[11] 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.

The interview results suggest that decision makers were much more impacted by the Test Bed experience, as compared to non–decision makers. After the Test Bed experience, decision makers reported, on average,

- More individual time spent on cyber security (2.78% of their time versus 1.61%)
- More money spent in the future on cyber security by their company (71.4% planned to increase spending after the Test Bed experience)

[11] 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.

Although attempts were made to tailor information based on the audience, it is likely that decision makers were both more able to consume the information presented during the Cyber Test Bed and had more of a stake in the outcome given that all or part of their role (and performance evaluations) involved effectively and efficiently managing the cyber security of their companies. One takeaway from the Test Bed is that 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.

Looking to the future, 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 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).

Appendix A: Cyber Test Bed Modules

Threat Briefing I - Discussed the various threats that companies can face as well as malicious attackers, their origin and types of exploits.

Asset Protection Training I - Discussed asset protection and various controls / countermeasures that can be implemented to protect assets.

Company Wide Introduction Video - Addressed an overview of cyber security and client participation in the test bed; this participation will help to strengthen the nation's economic an national security of the country.

Threat Briefing II – More in-depth briefing that targets attackers, their motivations and the types of businesses and technologies of interest that are targeted for exploit.

1st Cyber Newsletter – Newsletters addressed various security topics such as password protection, cloud security and financial Industry cyber threats.

2nd Cyber Newsletter - Newsletters addressed various security topics such as password protection, cloud security and financial Industry cyber threats.

Asset Protection Training II – Policy Briefing - More focused briefing that was geared towards management. During this briefing, policy framework was discussed and management was given the Policies and Procedures Templates.

3rd Cyber Newsletter - Newsletters addressed various security topics such as password protection, cloud security and financial Industry cyber threats.

Tools and Training – LanGuard / Mandiant / CCSAR tools were installed and utilized to determine the security economic posture. Results were communicated during the Threat II Briefing.

Threat Briefing III / Final Points – Reviewed key points for each of the asset protection areas as well as helping company employees see their role in protecting assets.

Review & Wrap Up – Included in the Threat III Briefing or in the Final Points.

Appendix B: Pre-Cyber Test Bed Questionnaire

Introduction

This interview is in support of a study being funded by the National Preparedness and Programs Directorate (NPPD) within the Department of Homeland Security (DHS). We are here today representing RTI International. RTI International is an independent, nonprofit research institute based in Research Triangle Park, North Carolina. We have a long history of scientific achievement in many areas of research, including education and training, surveys and statistics, advanced technology, and international development, economic and social policy.

RTI International and Applied Research Associates (ARA) will be implementing a set of intervention strategies with your company and several others in order to improve the level of cyber security you have in place based on increasing your knowledge of cyber security threats and available solutions. This interview is aimed at identifying your current knowledge, perceptions, attitudes and behaviors related to cyber security.

Do you have any questions before we begin?

Section 1: Background Questions

Your responses to the questions in Section 1 will help us understand your role at your company and who makes cyber security decisions at your company.

[ALL ANSWER]

1. What is your role at your company?
   - ☐ President / Chief Executive Officer
   - ☐ Chief Technical Officer
   - ☐ Chief Information Officer
   - ☐ Head of IT
   - ☐ Head of IT Security
   - ☐ Other (_____)

[ALL ANSWER]

2. How much time do you personally spend on cybersecurity related activities as a percent of your time?
   _____ %

[ALL ANSWER]

3. What is your involvement in cyber security decision making? (check all that apply)
   - ☐ I select and purchase security hardware
   - ☐ I select and purchase security software
   - ☐ I install and maintain hardware
   - ☐ I install and maintain software
   - ☐ I implement security policies
   - ☐ I implement security procedures
   - ☐ I help solve security issues that arise
   - ☐ I am not involved in cyber security decision making at all

[ALL ANSWER]

4. Who is the primary decision maker (or final approver) regarding cybersecurity investments?
   - ☐ CEO
   - ☐ CTO
   - ☐ CIO
   - ☐ Head of IT
   - ☐ Head of Risk Management
   - ☐ Other (_____)
   - ☐ Don't know

[ALL ANSWER]

5. How are IT security decisions made in your company? Please describe the process from your perspective. Who is involved? How are differences of opinion resolved? Etc.

   _____
   _____
   _____

Section 2: Cyber Security Perceptions

Your responses to the questions in Section 2 will help us understand how you view cyber security.

[ONLY EXECUTIVES AND IT STAFF ANSWER]

6. For each of the following types of security, please indicate any policies/procedures that you have in place:

	Documented Policy(ies)	**Access Restrictions**	**Employee Training**	**Other**
Cyber Security				
Intellectual Property Security				
Physical Security				
Personal Security				

If you selected "Other", please explain.

_____
_____
_____

[ONLY EXECUTIVES AND IT STAFF ANSWER]

7. Do you have contingency plans do you have in place e.g., for loss of power, network connectivity, etc.?
   - ☐ Yes
   - ☐ No

If YES, please describe.

_____
_____
_____

[ALL ANSWER]

8. Please define what you think cyber security means? _____
_____
_____

[ALL ANSWER]

9. How worried are you about cybersecurity on a scale of 1 to 10?

1 2 3 4 5 6 7 8 9 10

[ALL ANSWER]

10. What in particular are you concerned about regarding cyber security? (please rank)

☐ Loss of data / intellectual property
☐ Loss of customers / impact on reputation to the company
☐ Productivity loss associated with cyber attack / breach
☐ Other (_____)

[ALL ANSWER]

11. Do you believe that your company spends the appropriate amount of money and time on cyber security?

☐ Yes
☐ No
☐ Don't know how much time / money we spend

[ONLY EXECUTIVES AND IT STAFF ANSWER]

12. How did you arrive at your current level of spending? In the list below, for any factor that affects your cyber security spending, please rank them in terms of their relative importance (beginning with "1" for the factor that most influences your current level of spending on security) and write in any other factors as appropriate.

☐ We conducted a cost-risk calculation: _____
☐ Our vendor suggested a certain level: _____
☐ Our client requested a certain level of security: _____
☐ We spent enough to meet regulatory requirements: _____
☐ Internal or external audit suggested certain level: _____
☐ We heard about security threats in the news (e.g., media attention): _____
☐ We added security in response to internal security compromise: _____
☐ We spent as much as we could based on budget: _____
☐ I do not know: _____
☐ Other (_____): _____

Please explain briefly.

_____
_____
_____

[ONLY EXECUTIVES AND IT STAFF ANSWER]

Corporations often make decisions based on the relative priorities of key issues. The following questions ask you to compare the importance of network security with other priorities. Please answer to the best of your ability. There are no right or wrong answers.

[ONLY EXECUTIVES AND IT STAFF ANSWER]

13. Please characterize your organization's strategy regarding the tradeoff between ***network security*** *and* ***network performance*** using a response scale from 1 to 10 (10 = security is always more important, regardless of performance effects; 1 = network performance is always more important, regardless of security concerns).

1 2 3 4 5 6 7 8 9 10

[ONLY EXECUTIVES AND IT STAFF ANSWER]

14. Please characterize your organization's strategy regarding the tradeoff between ***network security*** *and* ***convenience for users*** using a response scale from 1 to 10 (10 = security is always more important, regardless of convenience effects; 1 = convenience is always more important, regardless of security concerns).

1 2 3 4 5 6 7 8 9 10

[ONLY EXECUTIVES AND IT STAFF ANSWER]

15. Please respond to the following statements using a response scale of 1 to 10 to quantify the extent to which your organization adheres to the following IT security strategies (10 = we always adhere to this strategy, 1 = we never adhere to this strategy).

"Our strategy toward IT security is proactive – we try to anticipate security compromises and to build in safeguards to prevent them."

1 2 3 4 5 6 7 8 9 10

"Our strategy toward IT security is reactive – we try to be as flexible as possible so that we can deal with any unexpected security compromises."

1 2 3 4 5 6 7 8 9 10

"Our strategy toward IT security is large mandated, by regulation(s), customer requirements, etc., therefore, we have little control in our strategy."

1 2 3 4 5 6 7 8 9 10

[ALL ANSWER]

16. Who do you think is attacking (cyber attacking) your company or might attack your company?

☐ Our competitors (U.S.)
☐ Our competitors (outside U.S.)
☐ Non-U.S. Governments (China or Russia)
☐ Criminals seeking data to sell
☐ Criminals seeking payment to desist
☐ Attackers seeking recognition/enjoyment
☐ Other (_____)

[ALL ANSWER]

17. Do you believe any of the following factors/entities are *increasing* the threat of cyber security to your organization?

- ☐ Security built in by my IT vendors
- ☐ Security of my suppliers
- ☐ Security of my customers/clients
- ☐ Security of my Internet service provider (ISP)
- ☐ Security of common websites
- ☐ Security of some home internet users
- ☐ Other (_____)

[ONLY EXECUTIVES AND IT STAFF ANSWER]

18. How do your company's ***downstream customers'*** levels of IT security affect your IT security decisions?

_____
_____ _____

[ONLY EXECUTIVES AND IT STAFF ANSWER]

19. How do your company's ***upstream suppliers'*** levels of IT security affect your IT security decisions?

_____
_____ _____

[ONLY REGULAR STAFF ANSWER]

20. In your opinion, which of the following statements best describes "malicious software" (malware), such as viruses, spyware, etc? Check only one.

- ☐ Software that is unintentionally poor (or buggy)
- ☐ Software that is intentionally designed to annoy you
- ☐ Software that is intentionally designed to support criminal activities (such as stealing your personal information)
- ☐ Don't know

[ONLY REGULAR STAFF ANSWER]

21. In your opinion, which of the following statements best describes the impact malware has on your work computer? Check only one.

- ☐ Malware causes problems similar to other types of buggy software
- ☐ Malware does not harm your computer, instead it typically steals personal information
- ☐ Malware causes a variety of annoying problems with your computer (crashes, popups that wont go away, etc)

[ONLY REGULAR STAFF ANSWER]

22. In your opinion, which of the following statements best describes the way malware gets on your computer? Check only one.

- ☐ Malware gets on your computer the same way other types of buggy software gets on your computer, by manually installing it.
- ☐ Malware gets on your computer when you don't follow good computer habits (you visit suspicious websites or open suspicious e-mails)
- ☐ Malware can get on your computer in a variety of ways without you even knowing it.

[ONLY REGULAR STAFF ANSWER]

23. In your opinion, which of the following statements best describes the primary purpose of most malware? Check only one.

☐ Malware is used to gather information for identity theft
☐ Malware is used to cause mischief or to annoy people
☐ Malware is used to gain fame among other virus creators
☐ Malware has no purpose because it is just unintentionally poor software

[ONLY REGULAR STAFF ANSWER]

24. Who is typically the target of malware?

☐ Everyone, including people like me
☐ People with wealth and influence
☐ Businesses or other organizations
☐ Malware has no targets

[ONLY REGULAR STAFF ANSWER]

25. Can you avoid getting a virus?

☐ Yes
☐ No

Section 3: Cyber Security Knowledge

Your responses to the questions in Section 3 will help us understand your individual and your company's general knowledge of cyber security threats and solutions.

[ONLY EXECUTIVES AND IT STAFF ANSWER]

26. How often are you informed (by other staff, an external vendor, or software you manage) of an attack on your company – e.g., DDoS attack, network probe, etc.?

☐ All the time
☐ Most of the time
☐ Some of the time
☐ Rarely
☐ Never

26a. If greater than "Never", how confident are you that your company is aware when you're being attacked? (between 0-100%)

_____ % confident

[ONLY EXECUTIVES AND IT STAFF ANSWER]

27. On a scale from 0% to 100%, what is your perception of the likelihood that your company will be attacked by a cyber criminal (inside or outside the company) in the next year?

    _____ % chance

    27.a If greater than 0%, how likely is it that you will have an attack in the next year that will cost you
    … greater than $5,000 in costs or losses? _____ % chance
    … greater than $10,000 in costs or losses? _____ % chance
    … greater than $20,000 in costs or losses? _____ % chance
    … greater than $50,000 in costs or losses? _____ % chance

[ONLY EXECUTIVES AND IT STAFF ANSWER]

28. Which statement best describes your knowledge of potential solutions available for all potential security threats to your company?

    ☐ I know what solutions are available for all threats
    ☐ I know what solutions are available for most threats
    ☐ I know what solutions are available for some threats
    ☐ I know what solutions are available for a few threats
    ☐ I do not know what solutions are available for any threats

[ONLY EXECUTIVES AND IT STAFF ANSWER]

29. Do you know where go to get information about threats?

    ☐ Yes
    ☐ No

[ONLY EXECUTIVES AND IT STAFF ANSWER]

30. Do you know where to go for information on potential solutions?

    ☐ Yes
    ☐ No

[ALL ANSWER]

31. Who do you ask for cybersecurity advice?

    ☐ IT professional (support service)
    ☐ Vendor who you bought software/hardware from
    ☐ Your Internet service provider (ISP)
    ☐ A friend
    ☐ A family member
    ☐ Other (_____)

[ONLY EXECUTIVES AND IT STAFF ANSWER]

32. Where do you get INFORMATION when making IT security decisions – e.g., hardware, software, and services purchasing decisions, determining IT security procedures, and determining IT security user policies? In the table below, in each column, please indicate (with an "X") the resources you typically use for each security need. If resources that you do not use or use very infrequently, please indicate why in the columns to the right.[SHOW TABLE TO INTERVIEWEE]

Information Resources	**Hardware/ Software**	**Services**	**IT Security Procedures/ Activities**	**User Policies**	**If no columns checked to the left, why not? (select reason at right)**	**Have not heard of this source**	**Do not trust this source**	**Too expensive**	**Other (____ _____ _____)**
Government regulations									
Customer suggestions/ requirements									
Vendor suggestions/ advice									
NIST best practices									
ISO guidelines									
ANSI guidelines									
Security impact estimates (e.g., CSI/FBI survey)									
CERTs, SANS, etc.									
Conferences or trade publications									
Outside consultants									
Other organizations									
Information Resources	**Hardware/ Software**	**Services**	**IT Security Procedures/ Activities**	**User Policies**	**If no columns checked to the left, why not? (select reason at right)**	**Have not heard of this source**	**Do not trust this source**	**Too expensive**	**Other (____ _____ _____)**
External audits									
Internal audits									
Staff experience/training									
Internally collected/ calculated data (e.g., number of compromises, cost estimates, etc.)									
CEO/CTO/COO/etc. suggestion									
Other (_____)									
Other (_____)									

Section 4: Cyber Security Behaviors

Your responses to the questions in Section 4 will help us understand how your company responds to the potential of cyber security threats.

[ONLY EXECUTIVES AND IT STAFF ANSWER]

33. How much money did your company spend on IT security related labor, hardware, software in 2010?

    $ _____ (round to the nearest $10,000)
    _____ % (as a % of total IT spending)

[ONLY EXECUTIVES AND IT STAFF ANSWER]

34. How much do you believe your company lost in terms of employee productivity, product delays, Intellectual property losses, etc. in 2010?

    $ _____

[ONLY EXECUTIVES AND IT STAFF ANSWER]

35. Does your IT group record your IT security resources (e.g., the number of hours spent by IT staff) allocated toward the following specific activities? (*yes* or *no*)

    ☐ Installing new IT security measures: _____
    ☐ IT security staff education: _____
    ☐ Gathering information (e.g., from CERTs, SANS, Gartner, etc.): _____
    ☐ Testing IT security measures: _____
    ☐ Monitoring IT security status: _____
    ☐ Responding to IT security problems: _____
    ☐ Other (_____): _____

[ONLY EXECUTIVES AND IT STAFF ANSWER]

36. How much training do your IT staff receive each year on new cybersecurity technologies and threats?

    ☐ 20+ hours per year
    ☐ 15-19 hours per year
    ☐ 10-14 hours per year
    ☐ 5-9 hours per year
    ☐ 1-4 hours per year
    ☐ 0 hours per year

[ONLY EXECUTIVES AND IT STAFF ANSWER]

37. How much training do your regular staff receive on cybersecurity threats / policies?

    ☐ 5+hours per year
    ☐ 3-4 hours per year
    ☐ 1-2 hours per year
    ☐ 30 minutes per year
    ☐ 0 minutes/hours per year

[ONLY EXECUTIVES AND IT STAFF ANSWER]

38. What general cyber security tools / policies are in place at the network level for your company?

- ☐ Network level firewall
- ☐ Network level IDS/IPS
- ☐ Network level threat analysis
- ☐ Network level role / access management
- ☐ Host level antimalware
- ☐ Host level password policy (expires every _____ days/months)
- ☐ Other (_____)

[ONLY EXECUTIVES AND IT STAFF ANSWER]

39. How is cybersecurity compliance by staff monitored / enforced?

- ☐ Manually
- ☐ Automated tools

Please describe.

_____
_____
_____
_____

[ONLY REGULAR STAFF ANSWER]

40. Does your company provide you with any training / education on cyber security issues?

- ☐ Yes, monthly training required
- ☐ Yes, bi-annual training required
- ☐ Yes, annual training required
- ☐ Yes, training required when started job
- ☐ Yes, but it is optional
- ☐ No, training / education not offered

[ONLY REGULAR STAFF ANSWER]

41. Approximately how much time have you spent in the **past month** learning about cybersecurity threats or complying with company policies?

- ☐ None
- ☐ 30 minutes
- ☐ 1 hour
- ☐ 2 hours
- ☐ 3-4 hours
- ☐ 5-6 hours
- ☐ 7-8 hours
- ☐ 8 hours or more

[ONLY REGULAR STAFF ANSWER]

42. Approximately how much time have you spent in the **past year** learning about cybersecurity threats or complying with company policies?

☐ None
☐ 30 minutes
☐ 1 hour
☐ 2 hours
☐ 3-4 hours
☐ 5-6 hours
☐ 7-8 hours
☐ 8 hours or more

[ONLY REGULAR STAFF ANSWER]

43. Which of the following are actions you or your company take to secure your work computer?

	I do this	My company does this for me	Neither my company nor I do this	Don't know
Use anti-virus software				
Keep anti-virus updated				
Regularly scan computer with anti-virus				
Use security software (firewall, etc)				
Don't click on attachments				
Am careful downloading from websites				
Am careful which websites I visit				
Disable scripting in web and e-mail				
Use good passwords				
Keep patches up to date				
Turn off or hibernate computer when not in use				

[ONLY REGULAR STAFF ANSWER]

44. What are you most concerned (worried) about when using the internet? (Please check any/all you are worried about.)

☐ Someone stealing your personal information (e.g., passwords, social security number, other personal files)
☐ Criminals gaining access to your online banking information (e.g., credit card numbers, bank account numbers)
☐ Your computer crashing or hard drive being erased
☐ The government tracking you
☐ Having sensitive personal information released without your permission
☐ Other (_____)
☐ Not afraid of anything

[ONLY REGULAR STAFF ANSWER]

45. In the past, do you think you have had security problems with a work computer?

☐ Yes
☐ No
☐ Don't Know

[If YES, ask the following]

Please briefly describe these problems.
_____
_____
_____

45a. How much time have you spent trying to fix these problem(s)?
_____ hours over the past 2 years

45b. Did you ask your company IT staff for help?
☐ Yes
☐ No

[ONLY REGULAR STAFF ANSWER]

46. To your knowledge, has your work computer been infected by a virus or worm in the last year?

☐ Yes
☐ No
☐ Don't know what these are

[ONLY REGULAR STAFF ANSWER]

47. To your knowledge, has your work computer been infected by any spyware?

☐ Yes
☐ No
☐ Don't know what these are

[ONLY REGULAR STAFF ANSWER]

48. Before taking this survey, were you aware of the possibility that a person can remotely break into your work computer through the internet and could, without your knowledge, use it to send spam or attack other computers on the internet?

☐ Yes
☐ No

[ONLY REGULAR STAFF ANSWER]

49. How concerned are you that someone will break into your work computer through the internet and could, without your knowledge, use it to send spam or attack other computers on the internet?

☐ Very concerned
Somewhat concerned
☐ Not concerned at all

[ONLY REGULAR STAFF ANSWER]

50. How likely do you think it is that someone **has used** your work computer to send spam or attack other computers connected to the internet without your knowledge?

☐ Very likely
☐ Somewhat likely
☐ Somewhat unlikely
☐ Very unlikely
☐ I don't know

[ONLY REGULAR STAFF ANSWER]

51. How likely do you think it is that someone **could use** your work computer to send spam or attack other computers connected to the internet without your knowledge?

☐ Very likely
☐ Somewhat likely
☐ Somewhat unlikely
☐ Very unlikely
☐ I don't know

Section 5: Cyber Security Needs

Your responses to the questions in Section 5 will help us understand what you need to improve how you are able to manage potential cyber security threats.

[ONLY EXECUTIVES AND IT STAFF ANSWER]

52. What are the barriers to adoption of appropriate IT security technologies within your industry?

_____
_____
_____

[ONLY EXECUTIVES AND IT STAFF ANSWER]

53. Generally, how does your organization assess the effectiveness of the following components of your IT security strategy? (By effectiveness, we generally mean the ability to prevent security compromises, while still enabling user productivity through strong network performance.)
    - IT administrative procedures/practices: _____
      _____
      _____
    - IT security infrastructure components (hardware/software): _____
      _____
      _____
    - User policies/procedures: _____
      _____
      _____

[ONLY EXECUTIVES AND IT STAFF ANSWER]

54. To your knowledge, does your organization have all the necessary information to make the best decision on IT security investments?

    ☐ Yes
    ☐ No

    54a. If NO, what additional information could you use? _____
    _____
    _____

[ONLY EXECUTIVES AND IT STAFF ANSWER]

55. What would incentivize you to spend more on cyber security?

    _____
    _____
    _____
    _____

[ONLY EXECUTIVES AND IT STAFF ANSWER]

56. Is there anything else you'd like to tell us about cyber security at your company?

    _____
    _____
    _____
    _____

Section 6: Demographics Questions

Your responses to the questions in Section 6 will help us understand your personal background. Our research has shown that perception of technology varies greatly by the experience of the respondent. We would like to learn a little more about you so that we can examine this relationship between personal experience and knowledge and perceptions of the cyber threat.

[ALL ANSWER]

57. How old are you? _____

[ALL ANSWER]

58. What is the highest level of education that you have achieved?

- ☐ Some high school
- ☐ High school diploma
- ☐ Associates degree
- ☐ Some college
- ☐ College degree
- ☐ Masters degree
- ☐ Doctoral degree
- ☐ Professional degree (e.g., JD, MBA)

[ALL ANSWER]

59. How many children do you have?

- ☐ None (skip to #3)
- ☐ 1
- ☐ 2
- ☐ 3
- ☐ 4 or more

[ALL ANSWER]

60. In 2009 how much did all members of your household earn before taxes? This figure should include salaries, wages, pensions, dividends, interest, and all other income.

- ☐ None or less than $9,999
- ☐ $10,000-$49,999
- ☐ $50,000 -$99,999
- ☐ $100,000-$119,999
- ☐ $120,000-$149,999
- ☐ $150,000-$199,000
- ☐ $200,000 and over

[ALL ANSWER]

61. Are you a citizen of the United States?

- ☐ Yes
- ☐ No

[ALL ANSWER]

62. What is your race? Please check all that apply.

- ☐ White
- ☐ Black or African American
- ☐ American Indian or Alaska Native
- ☐ Asian Indian
- ☐ Chinese

- ☐ Filipino
- ☐ Japanese
- ☐ Korean
- ☐ Vietnamese
- ☐ Other Asian
- ☐ Native Hawaiian
- ☐ Guamanian or Chamorro
- ☐ Samoan
- ☐ Other Pacific Islander
- ☐ Some other race

[ALL ANSWER]

63. Have you ever served in the United States military?
    - ☐ Yes, have served on active duty after 9/11/01.
    - ☐ Yes, served in active duty but only before 9/11/01.
    - ☐ Yes, served in the Reserves or National Guard since 9/11/01 but never called up for active duty.
    - ☐ Yes, served in the Reserves or National Guard but only before 9/11/01 and never called up for active duty.
    - ☐ No, never served in the military

[ALL ANSWER]

64. Politically speaking, do you think of yourself as a REPUBLICAN, a DEMOCRAT, an INDEPENDENT, or something else?
    - ☐ Republican
    - ☐ Democrat
    - ☐ Independent
    - ☐ Something Else

[ALL ANSWER]

65. If you had to choose, would you rather have a smaller government providing fewer services, or a bigger government providing more services?
    - ☐ a **smaller** government providing **fewer** services
    - ☐ a **bigger** government providing **more** services

[ALL ANSWER]

66. How much of the time do you think you can trust the government in Washington to do what is right?
    - ☐ Just about always
    - ☐ Most of the time
    - ☐ Only Some of the Time
    - ☐ Never

[ALL ANSWER]

67. Some people say that most people can be trusted. Other's say you can't be too careful in your dealings with people. Which of these opinions comes closest to your own?

☐ Most people can be trusted
☐ You can't be too careful

Thank you for your participation in this survey. If you have any questions about this study or how your responses will be used, feel free to contact the RTI study manager, Charlotte Scheper at cscheper@rti.org or 919-485-5587.

Appendix C: Post-Cyber Test Bed Questionnaire

Introduction

This interview is in support of a study being funded by the National Preparedness and Programs Directorate (NPPD) within the Department of Homeland Security (DHS). We are here today representing RTI International. RTI International and Applied Research Associates (ARA) have implemented a set of intervention strategies with your company and several others in order to improve the level of cyber security you have in place based on increasing your knowledge of cyber security threats and available solutions. This interview is aimed at identifying how these intervention strategies have affected your cyber security knowledge, perceptions, attitudes and behaviors.

Do you have any questions before we begin?

Section 1: Background Questions

Your responses to the questions in Section 1 will help us understand your role at your company and who makes cyber security decisions at your company.

1. What is your role at your company?
   - ☐ President / Chief Executive Officer
   - ☐ Chief Technical Officer
   - ☐ Chief Information Officer
   - ☐ Head of IT
   - ☐ Head of IT Security
   - ☐ Other (_____)

2. How much time do you personally spend on cybersecurity related activities as a percent of your time?
   _____ %

3. What is your involvement in cyber security decision making? (check all that apply)
   - ☐ I select and purchase security hardware
   - ☐ I select and purchase security software
   - ☐ I install and maintain hardware
   - ☐ I install and maintain software
   - ☐ I implement security policies
   - ☐ I implement security procedures
   - ☐ I help solve security issues that arise
   - ☐ I am not involved in cyber security decision making at all

4. Who is the primary decision maker (or final approver) regarding cybersecurity investments?
   - ☐ CEO
   - ☐ CTO
   - ☐ CIO
   - ☐ Head of IT
   - ☐ Head of Risk Management
   - ☐ Other (_____)
   - ☐ Don't know

5. How are IT security decisions made in your company? Please describe the process from your perspective. Who is involved? How are differences of opinion resolved? Etc.

   _____
   _____
   _____

Section 2: Cyber Security Perceptions

Your responses to the questions in Section 2 will help us understand how you view cyber security.

6. For each of the following types of security, please indicate any policies/procedures that you have in place:

	Documented Policy(ies)	**Access Restrictions**	**Employee Training**	**Other**
Cyber Security				
Intellectual Property Protection				
Physical Security				
Personnel Security*				

*a *Personnel Security* includes three broad areas of security: trustworthiness, capability, and operationally safe environments. (1) Trustworthiness includes background investigation; physical, mental, and psychological qualifications; behavioral observation; and voluntary and continuing assessments. (2) Capability addresses education and experience; training (equipment-specific, initial, and ongoing); security awareness; and certification by examination. (3) Operationally safe environments addresses vulnerability and risk assessment; hierarchy; internal, external, and contractor/vendor audits and enforcement; emergency planning; control system access control; identification and authentication; and emergency communication

If you selected "Other", please explain.

_____
_____
_____

7. Do you have contingency plans in place e.g., for loss of power, network connectivity, etc.?
   - ☐ Yes
   - ☐ No

7a. If YES, what type of plan(s) do you have in place?
   - ☐ Loss of power
   - ☐ Network connectivity
   - ☐ Other (_____)

8. Please define what you think cyber security means. _____
   _____
   _____

9. How worried are you about cybersecurity on a scale of 1 to 10?

   1 2 3 4 5 6 7 8 9 10

10. What in particular are you concerned about regarding cyber security? (please rank)

    ☐ Loss of data / intellectual property
    ☐ Loss of customers / impact on reputation to the company
    ☐ Productivity loss associated with cyber attack / breach
    ☐ Other (_____)

11. Do you believe that your company spends the appropriate amount of money and time on cyber security?

    ☐ Yes
    ☐ No
    ☐ Don't know how much time / money we spend

Corporations often make decisions based on the relative priorities of key issues. The following questions ask you to compare the importance of network security with other priorities. Please answer to the best of your ability. There are no right or wrong answers.

12. Please respond to the following statements using a response scale of 1 to 10 to quantify the extent to which your organization adheres to the following IT security strategies (10 = we always adhere to this strategy, 1 = we never adhere to this strategy).

    "Our strategy toward IT security is proactive – we try to anticipate security compromises and to build in safeguards to prevent them."

    1 2 3 4 5 6 7 8 9 10

    "Our strategy toward IT security is reactive – we try to be as flexible as possible so that we can deal with any unexpected security compromises."

    1 2 3 4 5 6 7 8 9 10

    "Our strategy toward IT security is largely mandated, by regulation(s), customer requirements, etc., therefore, we have little control in our strategy."

    1 2 3 4 5 6 7 8 9 10

13. Who do you think is attacking (cyber attacking) your company or might attack your company?

    ☐ Our competitors (U.S.)
    ☐ Our competitors (outside U.S.)
    ☐ Non-U.S. Governments (China or Russia)
    ☐ Criminals seeking data to sell
    ☐ Criminals seeking payment to desist
    ☐ Attackers seeking recognition/enjoyment
    ☐ Organized criminality
    ☐ Terrorists

☐ Nation states
☐ Other (_____)

14. Do you believe any of the following factors/entities are *increasing* the threat of cyber attacks to your organization?

☐ Security built in by my IT vendors
☐ Security of my suppliers
☐ Security of my customers/clients
☐ Security of my Internet service provider (ISP)
☐ Security of common websites
☐ Security of some home internet users
☐ Other (_____)

15. How do your company's ***downstream customers'*** levels of IT security affect your IT security decisions?
_____
_____ _____

16. How do your company's ***upstream suppliers'*** levels of IT security affect your IT security decisions?
_____
_____ _____

Section 3: Cyber Security Knowledge

Your responses to the questions in Section 3 will help us understand your individual and your company's general knowledge of cyber security threats and solutions.

17. How much do you believe your company lost in terms of employee productivity, product delays, Intellectual property losses, etc. in 2010?
$ _____

18. How often are you informed (by other staff, an external vendor, or software you manage) of an attack on your company – e.g., DDoS attack, network probe, etc.?

☐ All the time
☐ Most of the time
☐ Some of the time
☐ Rarely
☐ Never

18a. If greater than "Never", how confident are you that your company is aware when you're being attacked? (between 0-100%)
_____ % confident

19. On a scale from 0% to 100%, what is your perception of the likelihood that your company will be attacked by a cyber criminal (inside or outside the company) in the next year?
_____ % chance

19.a If greater than 0%, how likely is it that you will have an attack in the next year that will cost you

… greater than $5,000 in costs or losses? _____ % chance
… greater than $10,000 in costs or losses? _____ % chance
… greater than $20,000 in costs or losses? _____ % chance
… greater than $50,000 in costs or losses? _____ % chance

20. Which statement best describes your knowledge of potential solutions available for all potential security threats to your company?

☐ I know what solutions are available for all threats
☐ I know what solutions are available for most threats
☐ I know what solutions are available for some threats
☐ I know what solutions are available for a few threats
☐ I do not know what solutions are available for any threats

21. Do you know where go to get information about threats?

☐ Yes
☐ No

22. Do you know where to go for information on potential solutions?

☐ Yes
☐ No

23. Who do you ask for cybersecurity advice?

☐ IT professional (support service)
☐ Vendor who you bought software/hardware from
☐ Your Internet service provider (ISP)
☐ A friend
☐ A family member
☐ Other (_____)

Section 4: The Cyber Test Bed Experience

24. How valuable was the Cyber TB experience? On a scale of 1 to 10, where 1 indicates that the experience was not very valuable and 10 indicates that it was highly valuable, please indicate the value that you place on the experience.

1 2 3 4 5 6 7 8 9 10

25. Which pieces were most valuable in terms of the effect on your organization's cyber security strategy? Please rank the items below from those that were most valuable to those that were least valuable. If you plan equal value of some items, feel free to rank them the same.

☐ Threat Briefing I
☐ Asset Protection Training I
☐ Company Wide Introduction Video
☐ Threat Briefing II
☐ 1st Cyber Newsletter
☐ 2nd Cyber Newsletter
☐ Asset Protection Training II – Policy Briefing
☐ 3rd Cyber Newsletter
☐ Tools and Training
☐ Threat Briefing III
☐ Review & Wrap Up

26. How much time did you invest in the Cyber TB experience?

Your time (total number of hours): _____ hours
Total company investment (estimated total hours): _____ hours

27. How much money (if any) did your company invest during or after the Cyber TB experience (as a result of the Cyber TB experience)? F

Money invested during Cyber TB experience: $____ _____
Money invested post Cyber TB experience: $ _____

28. Understanding the value of the Cyber TB to companies such as yours helps the government determine what role they should play in cyber security. Knowing what you know now, prior to your participation, if the Cyber Test Bed were offered to you as a service for a price? Would you be willing to pay for Cyber Test Bed experience?

☐ Yes
☐ No

28a. If Yes, how much would you have been willing to pay?
$ _____

28b. Is this amount higher than you would have been willing to pay prior to participation? If so, how much higher?

_____
_____

29. Have you made changes recommended by the Cyber TB staff?

☐ Yes
☐ No

29a. If Yes, what recommended changes did you make? Please describe all.

_____
_____
_____
_____

30. Do you plan to make changes recommended by the Cyber TB staff?

☐ Yes
☐ No

30a. If Yes, what recommended changes will you make? Please describe all.

_____
_____
_____
_____

31. Are there areas where you made changes to your cyber security investments, policies, or procedures that differ from what the Cyber TB staff recommended?

☐ Yes
☐ No

31a. If Yes, which ones and when?

_____
_____
_____
_____

32. Moving forward, do you plan to increase or decrease your spending on cyber security?

☐ Increase
☐ Decrease
☐ Stay the same

32a. If increase or decrease, by how much do you plan to change your spending in the next year?

☐ Decrease 1-5%
☐ Decrease 6-10%
☐ Decrease 11-15%
☐ Decrease 16-20%
☐ Decrease 21-25%
☐ Decrease more than 25%

☐ Increase 1-5%
☐ Increase 6-10%
☐ Increase 11-15%
☐ Increase 16-20%
☐ Increase 21-25%
☐ Increase more than 25%

33. Moving forward, do you plan to record your IT security resources (e.g., the number of hours spent by IT staff) allocated toward the following specific activities? (*yes* or *no*)

☐ Installing new IT security measures: _____
☐ IT security staff education: _____
☐ Gathering information (e.g., from CERTs, SANS, Gartner, etc.): _____
☐ Testing IT security measures: _____
☐ Monitoring IT security status: _____
☐ Responding to IT security problems: _____
☐ Other (_____): _____

34. Moving forward, how much training will your IT staff receive each year on new cybersecurity technologies and threats?

- ☐ 20+ hours per year
- ☐ 15-19 hours per year
- ☐ 10-14 hours per year
- ☐ 5-9 hours per year
- ☐ 1-4 hours per year
- ☐ 0 hours per year

35. Moving forward, how much training will your regular staff receive on cybersecurity threats / policies?

- ☐ 5+hours per year
- ☐ 3-4 hours per year
- ☐ 1-2 hours per year
- ☐ 30 minutes per year
- ☐ 0 minutes/hours per year

36. Moving forward, what general cyber security tools / policies do you plan to implement at the network level for your company?

- ☐ Network level firewall
- ☐ Network level IDS/IPS
- ☐ Network level threat analysis
- ☐ Network level role / access management
- ☐ Host level antimalware
- ☐ Host level password policy (expires every _____ days/months)
- ☐ Other (_____)

37. Moving forward, how do you plan to monitor / enforce staff compliance with cybersecurity policies

- ☐ Manually
- ☐ Automated tools

Please describe.

_____
_____
_____
_____

38. Were you surprised by anything you learned during the Cyber TB?

_____
_____
_____
_____

39. Did you reprioritze any of your company objectives based on the Cyber TB experience?

_____
_____
_____
_____

40. Did you reprioritze any of your IT security objectives based on the Cyber TB experience?

_____
_____
_____
_____

41. Do you believe that other businesses would benefit from the Cyber TB experience?

☐ Yes
☐ No

a. If yes, what companies do you think would benefit most?

_____
_____
_____
_____

42. Do you believe that the government should pay to support the cyber security of companies or should private companies pay based on their own risk tolerance? Please explain your opinion.

_____
_____
_____
_____

Section 5: Cyber Security Needs

43. To your knowledge, does your organization have all the necessary information to make the best decision on IT security investments?

☐ Yes
☐ No

43a. If NO, what additional information could you use? _____
_____
_____

44. What would incentivize you to spend more on cyber security?

_____
_____
_____
_____

45. Is there anything else you'd like to tell us about cyber security at your company?

_____
_____
_____
_____

Thank you for your participation in this survey. If you have any questions about this study or how your responses will be used, feel free to contact the RTI study manager, Charlotte Scheper at cscheper@rti.org or 919-485-5587.