ECONOMIC ANALYSIS OF U.S TECHNOLOGY-BASED CYBER SECURITY INFRASTRUCTURE GAPS

The purpose of this study is to identify areas for improving the U.S. technology-based cyber security infrastructure (e.g., standards, standard policies and procedures, data, public-private partnerships for standardization and precompetitive technology development, and best practices) and to quantify the associated economic benefits. Below are a number of background questions that will allow us to use your survey responses appropriately, based on your role, industry and the size of your organization. These background questions are followed by a set of specific questions about your current cyber security activities and processes and the cost savings which your organization may see as a result of specific improvements in the cyber security infrastructure.

Your participation will help to ensure that new investments in the cyber security infrastructure (by both public agencies and private sector organizations) will be focused on areas that will have the greatest economic benefit to organizations like yours.

About Your Organization

Please characterize your organization's industry and size. Your responses to the following questions will only be used to aggregate with those of other organizations.

1. What is your title? _____

2. What industry are you in?

   Mining, Quarrying, and Oil and Gas Extraction
   Utilities
   Construction
   Manufacturing
   Wholesale Trade
   Retail Trade
   Transportation and Warehousing
   Information
   Finance and Insurance
   Real Estate and Rental and Leasing
   Professional, Scientific, and Technical Services
   Management of Companies and Enterprises
   Administrative and Support and Waste Management and Remediation Services
   Educational Services
   Health Care and Social Assistance
   Arts, Entertainment, and Recreation
   Accommodation and Food Services

Other Services (except Public Administration)
Public Administration

3. Where are you located (CITY, STATE)? _____

4. What was the approximate annual revenue or funding for your organization in 2010? Your best approximation will suffice.

   $0-9 million
   $10-49 million
   $50-99 million
   $100-249 million
   $250-499 million
   $500-999 million
   $1,000 million or more

5. Approximately how many people were employed by your organization in 2010?

   0-99
   100-249
   250-499
   500-999
   1,000-4,999
   5,000-9,999
   10,000-49,999
   50,000-99,999
   100,000 or more

6. Do you work on IT security for your entire organization?

   ___Yes
   ___ No

   6a. If No, for what percentage of your organization's IT security are you involved?

   _____ %

7. As a percentage of your organization's annual revenue, approximately what size is your organization's Information Technology budget? (circle one of the ranges below)

   1-3% 4-6% 7-9% 10-14% 15-19% 20-30% >30%

8. What percentage of your organization's IT budget do you estimate was allocated <u>specifically for IT security</u> in 2010?

   1-3% 4-6% 7-9% 10-14% 15-19% 20-30% >30%

9. Consider the resources allocated to your organization's IT security operations. Please estimate how your organization allocated, in percentage terms, its <u>IT security budget</u>

among the following four categories of IT security resources in 2010 *(Note: the total should equal 100%)*:

[CODING NOTE: Force to add up to 100%.]

Labor (full-time, part-time, temporary, and contract employees):_____ %
Capital (investment in software and hardware): _____ %
Services (vendors): _____ %
Other (please describe:_____) _____ %
100%

10. Approximately how many IT security employees, measured in terms of Full-Time Equivalent (FTE) employees, were working at your company in 2010? *(Note: as an example, if you had one employee spending 100% time on IT security and two part-time employees spending 50% time on IT security, you would have a total of 2 FTEs)*

_____ FTEs

Please review the following definitions before answering the next question:

Proactive investments: IT security spending on labor, capital, or services to help avoid incidents and breaches can be characterized as being *proactive.*

Reactive investments: IT security spending made in response to incidents (e.g., DDoS attacks, viruses, worms, malware, etc.) and breaches (e.g., lost/stolen/altered data) can be characterized as being *reactive*.

11. Based on the definitions above of proactive and reactive investments, please indicate the degree to which your organization's spending is more proactive or reactive using the sliding scale below.

[CODING NOTE: Insert sliding bar b/w Reactive & Proactive where total on each side equals 100%]
Reactive **Proactive**

12. As far as you are aware, did your organization participate in any industry consortia (e.g., serving on committees) or work on internal R&D projects specific to IT security standardization in 2010?

Place an x where applicable
Yes___ No___

12a. If yes, approximately how many person-hours did your organization expend in that year for these activities?
_____ hours

Specific IT Security Questions

Please review the following definitions before answering the next question:

IT Security Incident: An *incident* is defined as an attempted or successful compromise of a network/system that may result in loss of network/system integrity (e.g., a network is attacked by a DDoS attack, worm, virus. or other malware).

IT Security Breach: A *breach* is defined as a type of security *incident* in which the confidentiality or integrity of protected data or a network/system is compromised (e.g., data is stolen from a server).

13. Based on the definitions above, approximately how many IT security incidents did your organization observe **in 2010**?

    _____

    13a. What percentage of IT security incidents resulted in IT security breaches?

    _____ %

14. Below is a list of IT security activities and processes to which many organizations allocate their IT security budget. Please estimate the percentage of your IT security budget which you allocated to the following activities and processes **in 2010** *(NOTE: Please use the "Other" category for all activities and processes not listed in the table, such as authorization and administrative/management activities. The percentages should add to 100%)*.

    [CODING NOTE: Force to add up to 100%.]

Activity/Process	% of 2010 IT Security Budget
Responding to employee loss of physical equipment and electronic media	____%
Educating employees about IT security best practices	____%
Identifying potential threats by looking outside your organization (e.g. researching virus signatures)	____%
Gathering/reporting IT security metrics for internal use within the organization (e.g., for presentation to management and for efficiency/effectiveness analysis)	____%
Securing mobile devices	____%
Securing cloud-hosted data, applications, and infrastructure	____%
Manually monitoring and analyzing internal threat data (as opposed to using an automated	____%

system/process)	
Authenticating all system users	____%
Conducting audits and fulfilling compliance requirements	____%
Other	____%
	100%

15. How much would you be willing to pay for a 10% improvement in your IT security effectiveness (measured by the number of incidents you deal with each year)?

    $ _____

16. If your IT security effectiveness improved by 10%, by how much would you be able to decrease your reactive spending (e.g., responding to incidents/breaches such as DDoS attacks, viruses, worms, malware, etc.)? (Note: we recognize that some reactive costs will always be needed to address incidents outside your control, such as certain types of phishing attacks and DDoS attacks)

    _____ %

17. If your IT security budget increased by 10%, how would you spend the additional dollars If you had to allocate them among the activities and processes listed above?

    [CODING NOTE: Force to add up to 100%.]

Activity/Process	**What % of Your IT Security Budget <u>Increase</u> Would you Allocate to…**
Responding to employee loss of physical equipment and electronic media	____%
Educating employees about IT security best practices	____%
Identifying potential threats by looking outside your organization (e.g. researching virus signatures)	____%
Gathering/reporting IT security metrics for internal use within the organization (e.g., for presentation to management and for efficiency/effectiveness analysis)	____%
Securing mobile devices	____%
Securing cloud-hosted data, applications, and infrastructure	____%
Manually monitoring and analyzing internal threat data (as opposed to using an automated system/process)	____%
Authenticating all system users	____%
Conducting audits and fulfilling compliance requirements	____%
Other	____%
	100%

18. We would now like to present you with a series of hypothetical questions to determine the cost of improving each of the activities listed above in terms of effectiveness.

We are interested in whether it would be technically possible for your organization to achieve *on its own* a 10% increase in the IT security effectiveness (e.g., decrease in the number of incidents you have) of a set of activities, if you had a larger IT security budget. For each question below, enter an *x* in the applicable field. If you select *Possible*, enter your estimate of the required budget increase (as a percentage of your current spending in this area) to bring about a 10% increase in effectiveness of each activity. Assume that each of the activities and processes is independent of any other.

On our own, a 10% increase in effectiveness in…

[CODING NOTE: Only show the ones below for which percentages were entered greater than zero in Q14 above]

18a. … responding to employee loss of equipment and media is…
Possible ___ → and would require a ___% budget increase
Not possible ___
Don't know ___

18b. … educating employees about IT security best practices is…
Possible ___ → and would require a ___% budget increase
Not possible ___
Don't know ___

18c. … identifying potential threats by looking outside your organization is…
Possible ___ → and would require a ___% budget increase
Not possible ___
Don't know ___

18d. … gathering/reporting IT security metrics for internal use is…
Possible ___ → and would require a ___% budget increase
Not possible ___
Don't know ___

18e. … securing mobile devices is…
Possible ___ → and would require a ___% budget increase
Not possible ___
Don't know ___

18f. … securing cloud-hosted data, applications, and infrastructure is…
Possible ___ → and would require a ___% budget increase
Not possible ___
Don't know ___

18g. … manually monitoring and analyzing internal threat data is…
Possible ___ → and would require a ___% budget increase
Not possible ___
Don't know ___

18h. … authenticating all system users is…

Possible ___ → and would require a ___% budget increase
Not possible ___
Don't know ___

18i. … fulfilling auditing/compliance requirements specifically related to remediation and notification of incidents/breaches

Possible ___ → ___% increase required in budget
Not possible ___
Don't know ___

19. If mobile device security could be guaranteed, do you think the number of mobile devices used by your employees would increase? Enter an *x* in the applicable field

___Yes
___ No
___ Don't know

19a. If Yes, by how much? _____ % increase

20. If cloud computing security could be guaranteed, do you think your company would use more cloud storage and/or applications on the cloud? Enter an *x* in the applicable field

___Yes
___ No
___ Don't know

20a. If Yes, by how much?

_____ % increase in cloud storage (as a percent of GB used today)
_____ % increase in cloud application use (as a percent of traffic used today)

Additional Questions

21. Now we're interested in any ideas you may have. What infrastructures, standards, etc. would help your company improve security or reduce IT security-related spending?

_____
_____
_____
_____

22. Is there any additional information you would like to provide?

_____
_____
_____
_____

Contact Information

If you are interested in receiving a copy of the final report and/or would be willing to be contacted with additional follow-up questions, please provide your name and contact information and check each appropriate box below.

23. Name: _____

24. Organization Name: _____
25. Email address: _____

- ☐ Willing to be contacted with follow up questions
- ☐ Would like to receive copy of final report

NOTE: This questionnaire contains collection of information requirements subject to the Paperwork Reduction Act (PRA). Notwithstanding any other provisions of the law, no person is required to respond to, nor shall any person be subject to penalty for failure to comply with, a collection of information subject to the requirements of the PRA, unless that collection of information displays a currently valid OMB Control Number. The estimated response time for this questionnaire is 20 minutes. The response time includes the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this estimate or any other aspects of this collection of information, including suggestions for reducing the length of this questionnaire, to the National Institute of Standards and Technology, Attn., Greg Tassey, Gregory.tassey@nist.gov, Mail Stop 1060, 100 Bureau Drive, Gaithersburg, MD 20899, 301-945-2663. The OMB Control No. is 0693-0033, which expires on 10/31/2012.