Attachment B1

Cognitive Interview Guide Targeted Cognitive Testing for Cybersecurity for 2025 ABS

I. Introduction

The Annual Business Survey (ABS) collects and provides data on economic characteristics and demographics of U.S. businesses and owners. We are interested in gaining feedback from industry stakeholders to help us develop a module of survey questions about cybersecurity workers to place on a future cycle of the ABS.

About the Interviewee

Please briefly tell us about your business and your current position (for example, the number of employees, type of industry, and number of locations).

II. Cybersecurity

A. Definitions

A. How would you define cybersecurity work?

B. . We want to share a definition of cybersecurity. [Read definition below]

   a. Cybersecurity refers to any technology, measure, or practice aimed at preventing cyberattacks or mitigating their impact. It encompasses safeguarding individuals' and organizations' systems, applications, computer devices, sensitive data, and financial assets against threats such as computer viruses and sophisticated ransomware attacks.

   b. What do you think about this definition in relation to your businesses?

C. [All participants will be asked] Now, I'm going to share a definition of the cybersecurity workforce. [Read definition below]

   a. Cybersecurity workforce is made up of individuals whose primary focus is on cybersecurity as well as those in the workforce who need specific cybersecurity-related knowledge and skills to perform their work in a way that enables organizations to properly manage cybersecurity-related risks to the enterprise.

   b. How well does this definition describe the work of your business? [If needed] Tell me more.

B. In-House or Outsource Cybersecurity work (filter question)

Do you contract your cybersecurity work outside of your business (that is, the cybersecurity work for your business is done by an outside party or an external vendor who specializes in cybersecurity)?

[**If no**, then ask the following:]

How much did you pay for cybersecurity work in 2023? This includes salaries, benefits, equipment, software, training, consulting etc.

[After they provide a number] Can you tell me more about what expenses came to mind when determining that number (anything I didn't mention in the examples)?

[If time permitting, we will ask the following cost question] Has that cost increased over the past three years, so from 2020-2022? [If yes] Would you say it's increased a little or substantially?

Can you tell me about the reasons for establishing and maintaining the cybersecurity work in-house as opposed to outsourcing the work?

[Move to the next section “Occupation and duties”]

[**If yes**, then ask the following:]

Can you tell me about your business reasons for contracting your cybersecurity work to an outside vendor?

- [If necessary] Were there specific challenges that motivated you to go with an outside vendor?
- How easy or difficult was it to find a company/firm to do that work?
- Have you ever had in-house cybersecurity employees?
    - [If yes] Thinking about cost and level of expertise, how does contracting out this work compare to an in-house team at your business?

How much did you pay for your contracted/outsourced cybersecurity work in 2023? Can you tell me more about what this amount covers (the breakdown of services and deliverables)?

[Time permitting] Has that cost increased over the past three years, so from 2020-2022? [If yes] Would you say it’s increased a little or substantially?

Thinking about your business, how many contractors routinely performed cybersecurity activities in the last calendar year (2023)?

[The cybersecurity portion of the interview ends for businesses that contract out their cybersecurity work. Move to Section G of the guide]

C. Occupations and duties [Internal cybersecurity only]

Now I’d like to discuss some positions and duties of cybersecurity work for your feedback. [Share screen with position descriptions. Show position 1.] Here’s an example of one type of position, different titles and duties. Please read and let me know when you’ve finished.

Position 1: Chief Information Security Officer (CISO)/Information Security Manager

a) Examples of positions: head of cybersecurity, president of cybersecurity; cyber security manager, information systems security manager, Security Operation Center (SOC) manager, governance, risk, and compliance (GRC) manager

b) Example of duties: top security leader within an organization; oversee and govern the cybersecurity of a program, organization, system, or enclave; manages security teams, and ensures compliance with regulations

[After participant has read description, ask the following]

1. Do you have this position in your business?

   [If yes] How many people are in this type of position?

2. Do you agree or disagree with the examples of the position? Tell me more.

3. Do you agree or disagree with the duties of the position? Tell me more.

[Show position 2]. Here’s an example of another type of position, different titles and duties. Please read and let me know when you’ve finished.

Position 2: Cybersecurity Analyst/Engineer

a) Examples of positions: SOC analyst, analyst, digital forensics analyst, systems security analyst, information security analyst; cybersecurity architect, security architect, security engineer

b) Examples of duties: monitor an organization’s network and protect against cyber threats; evaluate security systems and take necessary actions to address vulnerabilities; design and implement security infrastructure, such as firewalls, intrusion detection systems, and access controls

[After participant has read description, ask the following]

4. Do you have this position in your business?

[If yes] How many people are in this type of position?

5. Do you agree or disagree with the examples of the position? Tell me more.

6. Do you agree or disagree with the duties of the position? Tell me more.

[Show position 3]. Here’s the last example of a cybersecurity position, different titles, and duties. Please read and let me know when you’ve finished.

Position 3: Penetration tester

a) Examples of positions: Pen tester, Ethical hacker

b) Examples of duties: Offensive security; perform simulated cyberattacks on a company's computer systems and networks to help identify security vulnerabilities and weaknesses

[After participant has read description, ask the following]

7. Do you have this position in your business?

[If yes] How many people are in this type of position?

8. Do you agree or disagree with the examples of the position? Tell me more.

9. Do you agree or disagree with the duties of the position? Tell me more.

Are there cybersecurity positions at your business that are not mentioned here? (Think about those where the primary job function requires the employee to spend at least 51% of their time performing cybersecurity duties). [If yes] Please tell me more about them.

[If not mentioned] What about privacy management roles and privacy engineering roles? Or Trust and Safety?

[Stop screenshare].

D. Job functions and skills [Internal cybersecurity only]

Which cybersecurity job functions and skills are the most important in your business?

Thinking about your business, how many employees routinely performed cybersecurity activities in the last calendar year (2023)?

How are your cybersecurity employees organized? Would you say:

- As one or a few working independently.
- As a small team.
- As multiple teams and/or centralized cybersecurity unit/department.
- As many working independently.

How easy/difficult was it to choose an answer? Are there answer choices that we are missing? [Probe to determine if there's a different way they would describe how their cybersecurity employees are organized]

E. Hiring qualified employees (Educational Training) [Internal cybersecurity only]

The Annual Business Survey may collect information on the educational background of cybersecurity employees at your business. Are you able to identify and report the level of education of your cybersecurity workers? [Note: We are not necessarily interested in the actual breakdown here. Rather, we want to know if they have access to this information and could and would report it on the ABS]. So, do you have access to information necessary to report how many [or what percent] have the following:

- High school diploma or GED
- Some college but no degree
- Postsecondary Issued Certificate
- Associate degree (AA, AS)
- Bachelor's degree (BA, BS)
- Master's degree (MA, MS)
- Professional degree (PhD, MD, JD, etc.)

Are you able to identify and report the number of cybersecurity workers that have a professional certification? [Note: We are not necessarily interested in the actual breakdown here. Rather, we want to know if they have access to this information and could and would report it on the ABS]. For example, would you be able to tell us how many [or what percent] of your cybersecurity workers have:

- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- CompTIA Security+
- Certified Ethnical Hacker (CEH)
- GIAC Security Essentials Certifications (GSEC)

Are you able to identify and report the number of your cybersecurity workers that have completed some work experience program (e.g., internships, apprenticeships, externships or similar programs)? These could be completed as part of a formal school program or a workplace program.

[Time permitting] When hiring employees or contractors for cybersecurity, can you rank the following in importance: education, professional certification, and experience?

[Time permitting] Is there a particular cybersecurity educational profile that businesses like yours are looking for, thinking about technical skills, knowledge, and experience?

F. Demographics [internal cybersecurity only]

Are you able to identify and report the demographic information about your business's cybersecurity employees? For example, race and ethnicity, gender, U.S. citizenship. [If no] Could/would you be able to find and provide that information?

[Time permitting] What demographics are important to consider when thinking about the cybersecurity workforce?

G. Cybersecurity and R&D

Please open the questionnaire that we emailed you. Once you have it open, please share your screen. Please read and answer the questions as if I were not here.

[P will complete questions 1-3 on the questionnaire. Shortened version below:]

1. During 2023, did this business do any of the following R&D activities? Include activities that:

a. Conducted activities aimed at acquiring new knowledge or understanding without specific immediate commercial applications or uses
b. Conducted activities aimed at acquiring new knowledge for solving a specific problem or meeting a specific commercial objective
c. Conducted systematic work, drawing on research and practical experience and resulting in additional knowledge, which is directed to producing new products or processes or to improving existing products or processes
d. Developed and tested goods, services, or processes that were derived from scientific research or technical findings
e. Developed software that advanced scientific or technological knowledge
f. Produced findings that could be published in academic journals or presented at scientific conferences
g. Applied scientific or technical knowledge in a way that has never been done before
h. Created new scientific or technical solutions that can be generalized to other situations
i. Conducted work to discover previously unknown technological facts, structures, or relationships
j. Conducted work to extend the understanding of scientific facts, relationships, or principles in ways that could be useful to others

2. What was the total cost (both direct and indirect) in 2023 for all the R&D activities reported as "Yes" in the above question?

Report dollar amount in thousands. If none, report zero.

Include:

- Salaries, wages, and fringe benefits
- Plant, machinery, and equipment, except that which was capitalized because it had an alternative future use
- Materials, supplies, software

- Rent and utilities
- Consultants and contractors
- Depreciation expense from plant, machinery, and equipment that was capitalized because it had an alternative future use

Exclude:

- Costs for routine product testing, quality control, and technical services unless they are an integral part of an R&D project
- Market research
- Efficiency surveys or management studies
- Literary, artistic, or historical projects, such as films, music, or books and other publications
- Prospecting or exploration for natural resources
- Capital expenditures (i.e., costs for construction or renovation of facilities).
- Payments/funds in excess of the actual cost of the research work performed (e.g., profits or fees)

Total Amount of R&D Costs __________________

3. What amount of the total R&D costs was for cybersecurity?

Total Amount of Cybersecurity R&D Costs __________________

[When P is finished answering and if they have reported any cybersecurity R&D costs]

How did you determine how much of your business' R&D investments were for cybersecurity only?

Tell us more about the types of cybersecurity R&D investments that came to mind.

[When P is finished answering and if they *did not* report any cybersecurity R&D costs] Just to confirm, none of the R&D costs were for cybersecurity?

Tell us more about how you arrived at that answer.

[If P says they don't know if or how much of R&D costs are for cyber] Would you be able to find and report information about cybersecurity R&D costs?

Closing

That's all the questions that we have for today. Is there anything else that we did not talk about today that we should be thinking about? [After discussion]. Thank you so much for your feedback and for your time today.