Disclaimer

This presentation provides results of exploratory research by the National Center for Science and Engineering Statistics (NCSES) within the U.S. National Science Foundation (NSF). This information is shared to inform interested parties of ongoing activities and to encourage further discussion. Views expressed are those of the presenters and not necessarily those of NCSES or NSF.

This product has been reviewed for unauthorized disclosure **of confidential information** under NCSES-DRN24-067.

The Census Bureau has reviewed this data product to ensure appropriate access, use, and disclosure avoidance protection of the confidential source data (Project No. P-P-7530157, Disclosure Review Board (DRB) approval numbers: CBDRB-FY25-ESMD001-005 and CBDRB-FY25-ESMD001-004

Using the Annual Business Survey to improve measurement of the U.S. cybersecurity workforce

Shelley Feuer[1], Gigi Jones[1], Michael Prebil[2], Karen Wetzel[2]

[1]National Center for Science and Engineering Statistics | U.S. National Science Foundation

[2]NICE | National Institute of Standards and Technology

FCSM 2024

The Digital Age Problem: Defending Our Data Against Cybersecurity Threats

- Cyberattacks target individuals, corporations, and governments
  - In 2023, 349 million people were affected by a data breach
  - Industry data breaches are predicted to be the costliest for the U.S., averaging $9.36 million per incident (2024)
- High demand for skilled and experienced cybersecurity professionals
  - "Cyber criminals need to be successful once, but cybersecurity professionals need to be right all the time."

CHIPS and Science Act (2022) Mandate: Cybersecurity Workforce Data Initiative

(§ 10317) NCSES, in coordination with NIST and other federal statistical agencies, shall establish a Cybersecurity Workforce Data Initiative (CWDI) that –

- Assesses the feasibility of providing nationally representative estimates and statistical information on the cybersecurity workforce
- Utilizes the NICE Framework or other frameworks, as appropriate
- Utilizes existing data on employer requirements and unfilled positions
- Consults key stakeholders
- Evaluates existing Federal survey data
- Evaluates administrative data
- Collects credential attainment and employment outcome data

About NICE

- Led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce
- A partnership between government, academia, and the private sector
- Established by the Cybersecurity Enhancement Act of 2014, Title IV

NICE Mission

To energize, promote, and coordinate a robust community working together to advance an integrated ecosystem of cybersecurity education, training, and workforce development.

Workforce Framework for Cybersecurity (NICE Framework)

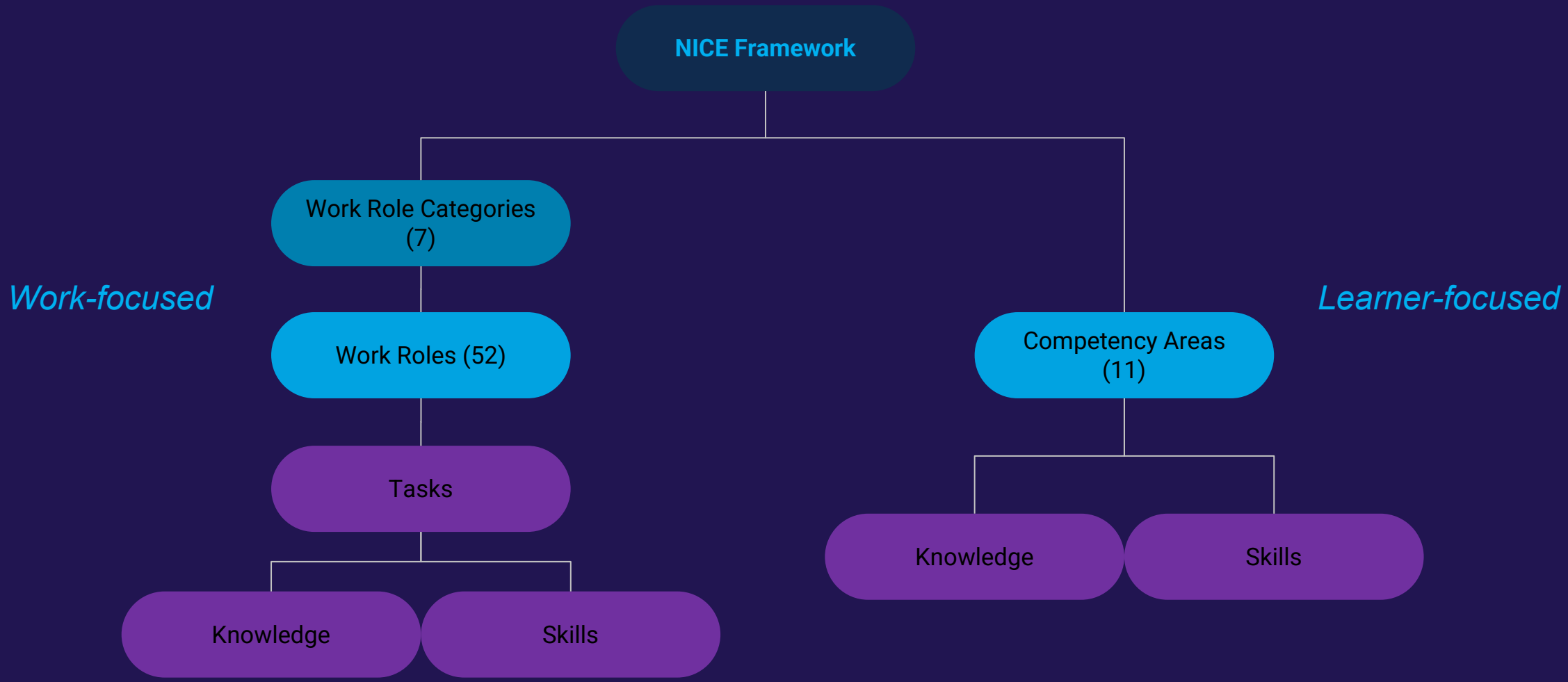
NIST SP 800-181r1 (2020) | NISTIR 8355 (2023) | Components v1.0.0 (2024)

- A **common language** to clearly describe what cybersecurity learners need to know
- A **modular, building-blocks approach** based on Task, Knowledge, and Skill (TKS) statements
- Defined **Work Roles** and **Competency Areas** for use in:
  - Career discovery
  - Education and training
  - Workforce planning and assessment
  - Hiring and career development

www.nist.gov/nice/framework

Credit: NICE

Structure of the NICE Framework



Credit: NICE

Drawing from the NICE Framework to Help with NCSES Survey Data Needs

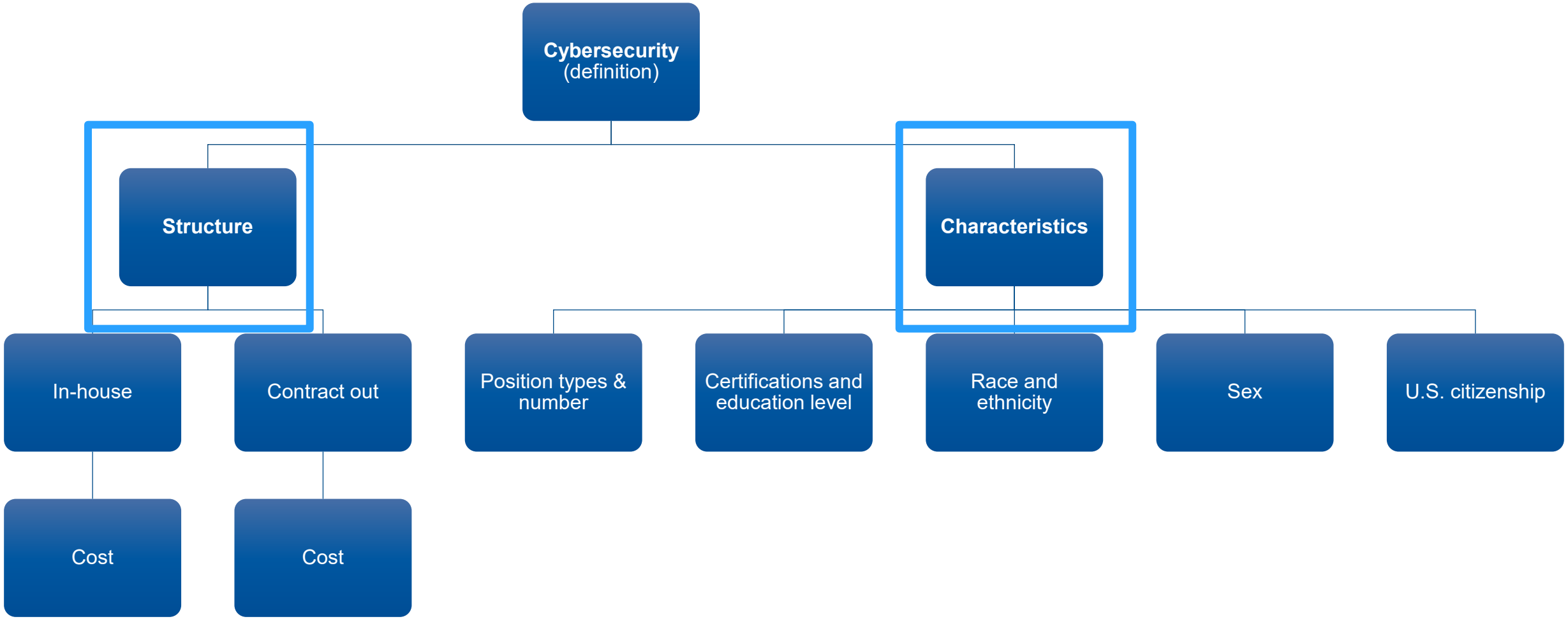
- Of the seven (7) Work Role Categories, NCSES was interested in testing and measuring the following from the business perspective:
  - Oversight and governance
  - Implementation and operation
  - Protection and defense
  - Investigation
- Interested in demographic information

Annual Business Survey (ABS)

An opportunity to develop a Cybersecurity module for 2025 ABS

- A mandatory survey conducted by NCSES and Census Bureau
  - Primary source of information on R&D among U.S.-based for-profit businesses with one to nine employees. Also collects data on innovation, technology, intellectual property, and financing from U.S.-based companies of all sizes.
- **Population size**: ~4.9 million employer companies
- **Sample size**: ~300K employer companies
  - Various sizes of less than 10 employees (microbusinesses) to over 2,500 employees (large business)
- **Sample frame**: U.S. Census Bureau Business Register (BR)
- Develop a module to provide essential industry data about U.S. employed cybersecurity workers

Cybersecurity areas of interest

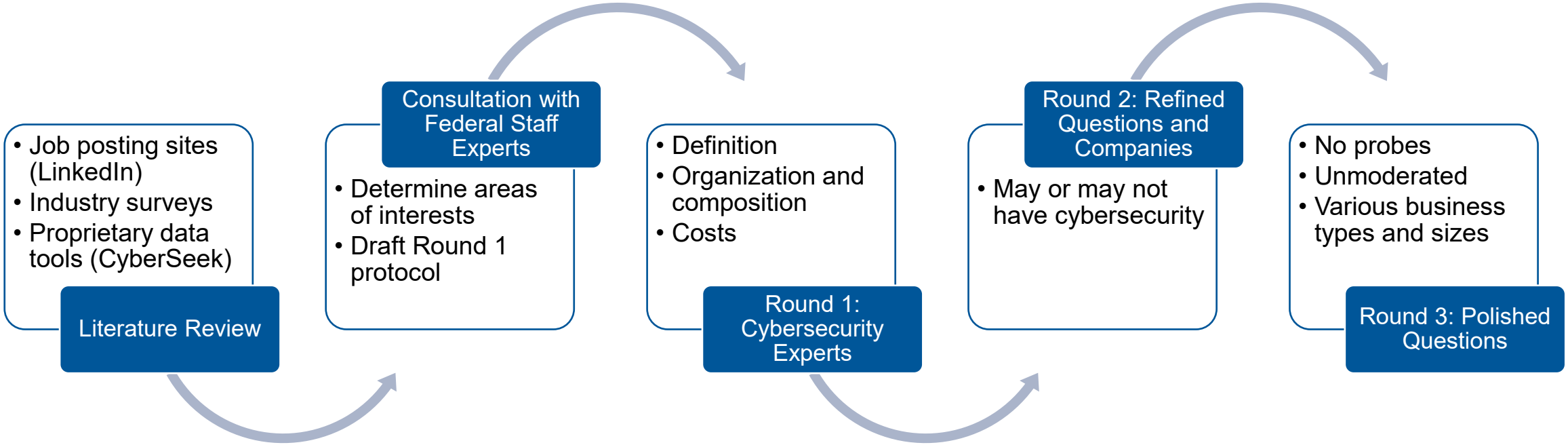


Methodology

- Three rounds of iterative cognitive testing to:
  - Determine how respondents (Rs) understand questions
  - Assess Rs' ability to answer specific questions and to identify areas of difficulty
  - Identify Rs' use of records or estimation strategies for answering specific questions
  - Evaluate and refine the survey questions

- Recommend questions and response options to be implemented in the 2025 ABS module

Methodology: Question development



Methodology: Sample

	Round 1: Cybersecurity Experts	Round 2: Businesses
N	10	13
Respondent roles	CEO, Founder, Chief Security Officer and other leadership positions	CFO, owner, operations director, controller, and accountant
Company types	technology consulting, specialty manufacturing, and nonprofits engaged in research and education	hospitality, food manufacturing, machine manufacturing, retail, nursing home, legal services
Total number of employees	<19 20–50 50–99 100–249	<19 20–50 50–99 100–249 250–500 500–999

Cybersecurity definition

Goal: To orient ABS respondents to questions about their cybersecurity procedures and employees

Round 1

- Rs presented with NIST definition:

> *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.*

FINDINGS

- Majority of Rs agreed with definition, offering few changes

Round 2

Question: Does this business use cybersecurity procedures either through your own staff or a third party?

In this context, cyber*security 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.*

- Yes
- No
- Don't know

FINDINGS

- Rs said definition is clear
- Majority answered yes
- Rs who said no were asked for reasons
  - Not required for type of business

How businesses conduct cybersecurity

Goal: To understand how businesses do cybersecurity (in-house staff or contract out)

Round 1

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)?

- Yes
- No

FINDINGS

- Rs reported cybersecurity conducted in-house
- Rs mentioned mix of in-house and outsourced would be most common
  - Not a binary yes or no question

Round 2

Question: Who does cybersecurity work for this business?

- We do it all IN-HOUSE
- We CONTRACT OUT to a third party
- A mix of IN-HOUSE and CONTRACTED OUT

FINDINGS

- Rs did not have trouble answering
- Some Rs reported in-house, some contract out, and some reported a mix of the two
  - Smaller businesses tend to contract out
- Reasons for contracting out:
  - Outside vendors have subject matter expertise
  - External testing is necessary to understand vulnerabilities (i.e., certain aspects of cybersecurity are better outsourced)

How much does cybersecurity cost?

Goal: Determine how much the business spends on cybersecurity and what's included in that cost

- **Question:** How much did the company spend on cybersecurity in 2023? *This includes salaries, benefits, equipment, software, training, consulting, etc.*
- **Question:** What does this amount cover? Can you provide the cost breakdown of services?
  - If a mix of in-house and contracted out, Rs were asked to think about each separately

FINDINGS

- **Round 1:** Rs could not provide an exact amount or an estimate; reported they could if they consulted others
  - Because Rs couldn't provide a total value, they could not provide the cost breakdown of services
- **Round 2:** Some Rs reported that they would consult with human resources (HR), payroll, etc., which would not be burdensome
- Rs who contract out reported they could not separate out the cost for cybersecurity from other information technology (IT) activities
  - For example, businesses receive one invoice from IT contractor that does not breakdown types of services

- More testing in Round 3 to gather more info about how and when businesses can provide these figures

In-house cybersecurity employees Round 1

Goal: Determine the number and type of cybersecurity employees in each business

- Questions and response options modeled after existing ABS questions

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

Question: 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

2022 ABS

F.9 Number of Employees and Design Activities

How many employees and/or contractors routinely performed design activities in the following years?

If none, report zero.

Number of Employees

2021 .....

2019 .....

F.10 Organization of Design Employees

How are the employees and/or contractors who routinely perform design activities organized?

Select all that apply.

- ☐ As one or a few working independently
- ☐ As a small team
- ☐ As multiple teams and/or centralized design unit/department

In-house cybersecurity employees

Round 1

FINDINGS

- Experts had difficulty answering; expressed confusion
- Reported combination of multiple teams, outsourced functions, overlap in roles
- Emphasized that all employees have a role in cybersecurity, not just IT teams
- Dependent on business size

- *NCSES Cybersecurity Workforce Data Initiative: Cybersecurity Workforce Definitions Report*
  - Core workforce
  - Adjacent workforce
- Based on percentage of work activities that align with NICE framework

Round 2

Question: How many employees does this business have who spend:

50% or more of their time on cybersecurity? [ ]

For 50%-or-more employees, cybersecurity is a critical component of their work role. Their primary focus is on cybersecurity and they need specific cybersecurity-related knowledge and skills to perform their work.

Some time on cybersecurity but less than 50%? [ ]

For less-than-50% employees, cybersecurity is a work activity but not a primary part of their regular work role.

FINDINGS

- Rs reported small numbers, few with employees who spend 50% or more time on cybersecurity duties
- Rs reported that they would consult records or colleagues

In-house positions Round 1

Position	Example of Positions	Example of Duties
1.Chief Information Security Officer (CISO) / Information Security Manager ***Oversight and Governance***	Head of cybersecurity, president of cybersecurity, cyber security manager, information systems security manager, Security Operation Center (SOC) manager, governance risk and compliance (GRC) manager	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
2. Cybersecurity Analyst / Engineer ***Protection and Defense Implementation and Operation***	SOC analyst, analyst, digital forensics analyst, systems security analyst, information security analyst, cybersecurity architect, security architect, security engineer	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
3. Penetration tester ***Investigation***	Pen tester, ethnical hacker	Perform simulated cyberattacks on a company's computer systems and networks to help identify security vulnerabilities and weaknesses

In-house positions: CISO/Information Security Manager

Round 1

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

FINDINGS

- Positions common and examples of duties match them
  - For example, head of cybersecurity and cyber security manager well understood
- Development, incident response, and risk management as additional duties

Round 2

Question: Please indicate the number of employees in each of the following cybersecurity positions:

Chief Information Security Officer (CISO) / Information Security Manager (e.g., head of cybersecurity, cyber security manager)	
Cybersecurity Analyst / Engineer (e.g., SOC analyst, systems security analyst, information security analyst, security engineer)	
Vulnerability Analyst (e.g., pen tester, ethnical hacker, red hat, threat intelligence)	
Other (please specify position and number of employees)	

In-house positions: Cybersecurity Analyst/Engineer

Round 1

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

FINDINGS

- Positions common and examples of duties match them
- Digital forensics analyst too specific

Round 2

Question: Please indicate the number of employees in each of the following cybersecurity positions:

Chief Information Security Officer (CISO) / Information Security Manager (e.g., head of cybersecurity, cyber security manager)	
Cybersecurity Analyst / Engineer (e.g., SOC analyst, systems security analyst, information security analyst, security engineer)	
Vulnerability Analyst (e.g., pen tester, ethnical hacker, red hat, threat intelligence)	
Other (please specify position and number of employees)	

In-house positions: Vulnerability Analyst and Other

Round 1

Position 3: Penetration tester

a) Examples of positions: PEN tester, Ethical hacker

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

FINDINGS

- Vulnerability analyst more appropriate for position
  - A pen tester is type of vulnerability analyst
- Add threat intelligence to example positions
- Add red hat to example positions

- Overall Rs suggested an “Other” category

Round 2

Question: Please indicate the number of employees in each of the following cybersecurity positions:

Chief Information Security Officer (CISO) / Information Security Manager (e.g., head of cybersecurity, cyber security manager)

Cybersecurity Analyst / Engineer (e.g., SOC analyst, systems security analyst, information security analyst, security engineer)

Vulnerability Analyst (e.g., pen tester, ethnical hacker, red hat, threat intelligence)

Other (please specify position and number of employees)

Demographics: Education and Certifications

Goal: To understand the demographic makeup of the cybersecurity workforce

Round 1: Education before credentials

Question: What is the highest degree or level of school that your cybersecurity employees have completed? *Provide the number of employees for each.*

- 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.)

FINDINGS

- Rs commented that certifications are more important than education level
  - Didn't realize next question would be about certifications
- Many types of certifications but Rs commented that examples presented were common

Round 2: Switch order

Question: How many employees who worked in cybersecurity have each of the following certifications? *Provide the number of employees for each.*

- Certified Information Systems Security Professional (CISSP)
- Certified Information Systems Auditor (CISA)
- CompTIA Security+
- Certified Ethical Hacker (CEH)
- GIAC Security Essentials Certifications (GSEC)
- Other, please specify

FINDINGS

- No comments on order
- Rs would typically have to consult with HR or other records answer

Demographics: Race and Ethnicity, Gender, Citizenship

Question: What is the race and/or ethnicity of the cybersecurity employees? *Provide the number of employees for each.*

- American Indian or Alaska Native
- Asian
- Black or African American
- Hispanic or Latino
- Middle Eastern or North African
- Native Hawaiian or Pacific Islander
- White
- More than one race or ethnicity

Question: What is the gender of the cybersecurity employees? *Provide the number of employees for each.*

- Male
- Female
- Transgender and/or nonbinary

Question: What is the U.S. citizenship status of the cybersecurity employees? *Provide the number of employees for each.*

- U.S. Citizen
- Permanent U.S. Resident Visa (Green Card)
- Temporary U.S. Resident Visa
- Other, please specify

FINDINGS

- Rs with small teams were able to answer some visible demographics (e.g., all white males)
- Rs would typically have to consult with HR or other records
- Citizenship Question: Rs mention employees based outside U.S.
- Unique challenges of asking workforce demographics on establishment survey
  - How to phrase for proxy reporting on more than one person
  - Rs answer demographic questions about business owners, so more demographic info could seem repetitive and burdensome
  - Larger businesses may have hundreds of cybersecurity employees to report

Summary: Methodological Approach

Summary

How?

- How businesses employ cybersecurity procedures (outsource, in-house, mix) depends on the size of the business

Cost

- Ease of reporting total cost and breakdown depends on how businesses do cybersecurity
- Often requires consulting people in other departments, records, accounting, etc.

Size Matters

- Smaller businesses tend to outsource all IT-related work
  - Rs who complete the ABS may not be able to provide cybersecurity-only costs
- Medium and large businesses tend to only outsource some (if any) cybersecurity services
  - In-house more likely able to provide information about cost and breakdown and number of cybersecurity employees

Who?

- Obtaining a count of in-house cybersecurity employees requires further defining using NICE framework
  - Number of employees who spend 50% or more of their time on cybersecurity (i.e., core, primary work role)
- Collecting demographic info about cybersecurity employees on ABS can be challenging (proxy reporting on many people)
  - Awkward question wording
  - Burdensome

Conclusion and Future Directions

- ABS cybersecurity module can fill critical workforce-information gaps
- Provide essential industry data about employed U.S. cybersecurity workers
  - How businesses implement cybersecurity measures
  - Who does cybersecurity work
- Augment NICE Framework's data assets (CyberSeek)
- Meet the CHIPS Act mandate

Future directions

- Round 3: Analyze results from unmoderated testing of refined questions
  - Debriefing session with select respondents
- Finalize module for potential inclusion on ABS 2025

Acknowledgements

- U.S. Census Bureau colleagues

  Hilary Steinberg

  Katie Beardall

  Temika Holland

- NCSES CWDI Working Group

  Ruiyi Li

  Daniela Oliveira

  Vrinda Nair

  Kelly Phou

  Julia Milton

  Amber Levanon Seligson

  Danielle Taylor

  John Finamore

https://ncses.nsf.gov/about/cybersecurity-workforce-data-initiative

Shelley Feuer (sfeuer@nsf.gov)
Gigi Jones (gijones@nsf.gov)
Michael Prebil (michael.prebil@nist.gov)
Karen Wetzel (karen.wetzel@nist.gov)