



Cybersecurity Workforce: How to go from  
Minding the Gap to Closing the Gap

**NICE** | Conference  
and Expo  
**2019**  
NATIONAL INITIATIVE FOR  
**CYBERSECURITY** EDUCATION

# Speakers

---



**Meredith Ward**

Director, Policy & Research  
NASCIO



**Andy Hanks**

CISO  
State of Montana



**Tara Mahoutchian**

Senior Manager, Human Capital  
Deloitte



# The National Picture

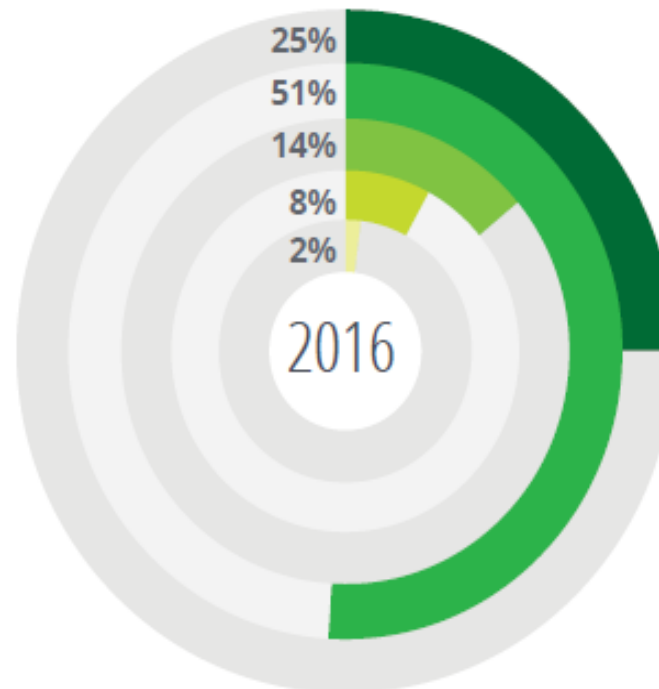
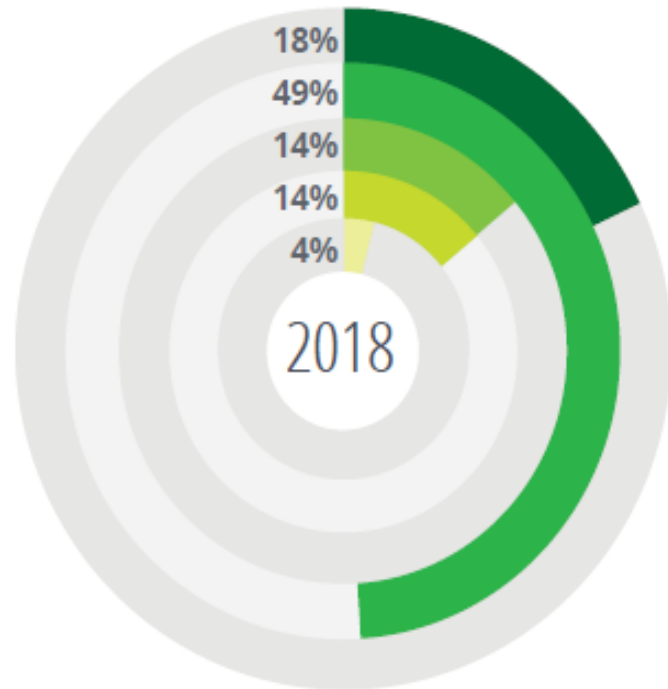
---



# Talent crisis

Most enterprise cybersecurity team consists of only 6-15 FTEs

■ 1-5 full-time equivalents ■ 6-15 full-time equivalents ■ 16-25 full-time equivalents  
■ 26-50 full-time equivalents ■ > 51 full-time equivalents



Compared to



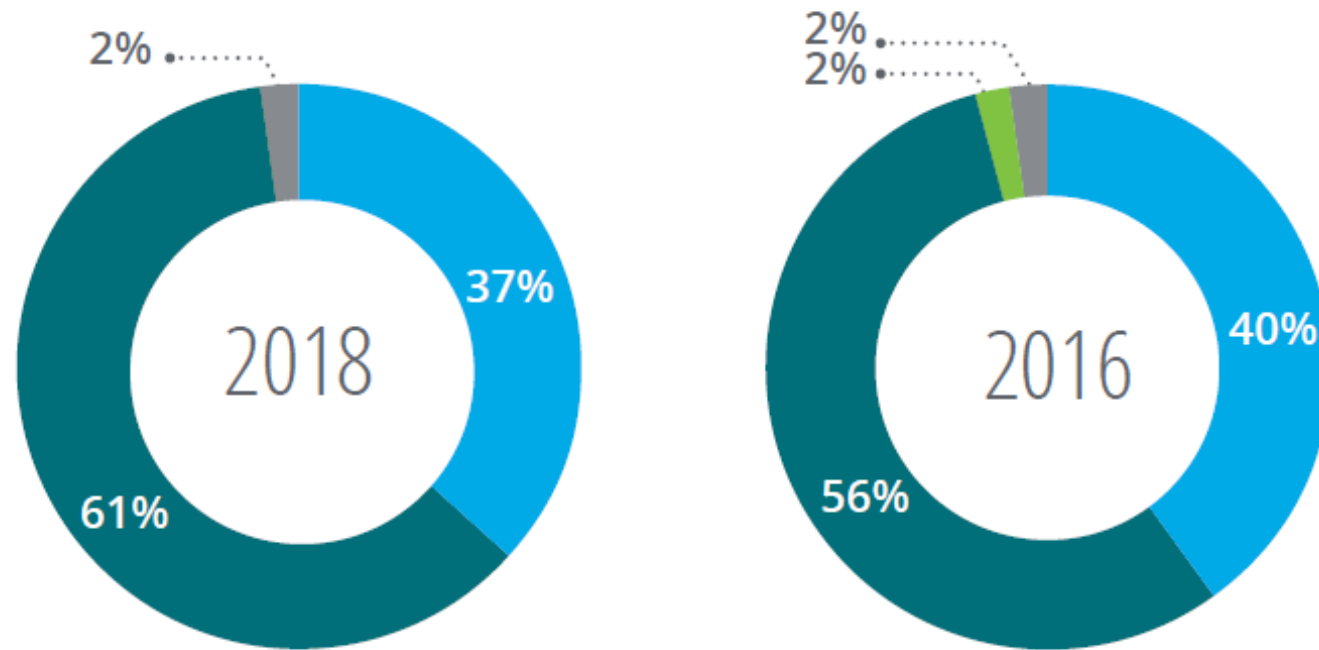
Survey question: How many dedicated cybersecurity professionals does your enterprise security office employ? (49 respondents)

\* Financial services institutions similar in size to an average state.

# Talent crisis

## Thirty state CISOs acknowledge they face a cyber competency gap

- Staff has the required competencies
- Staff has gap in competencies
- Not applicable/do not know
- Other



Survey question: Do your internal cybersecurity professionals have the required competencies (i.e., knowledge, skills, and behaviors) to handle existing and foreseeable cybersecurity requirements? (49 respondents)

# Talent crisis

## Top barriers to hiring, developing and retaining cyber talent

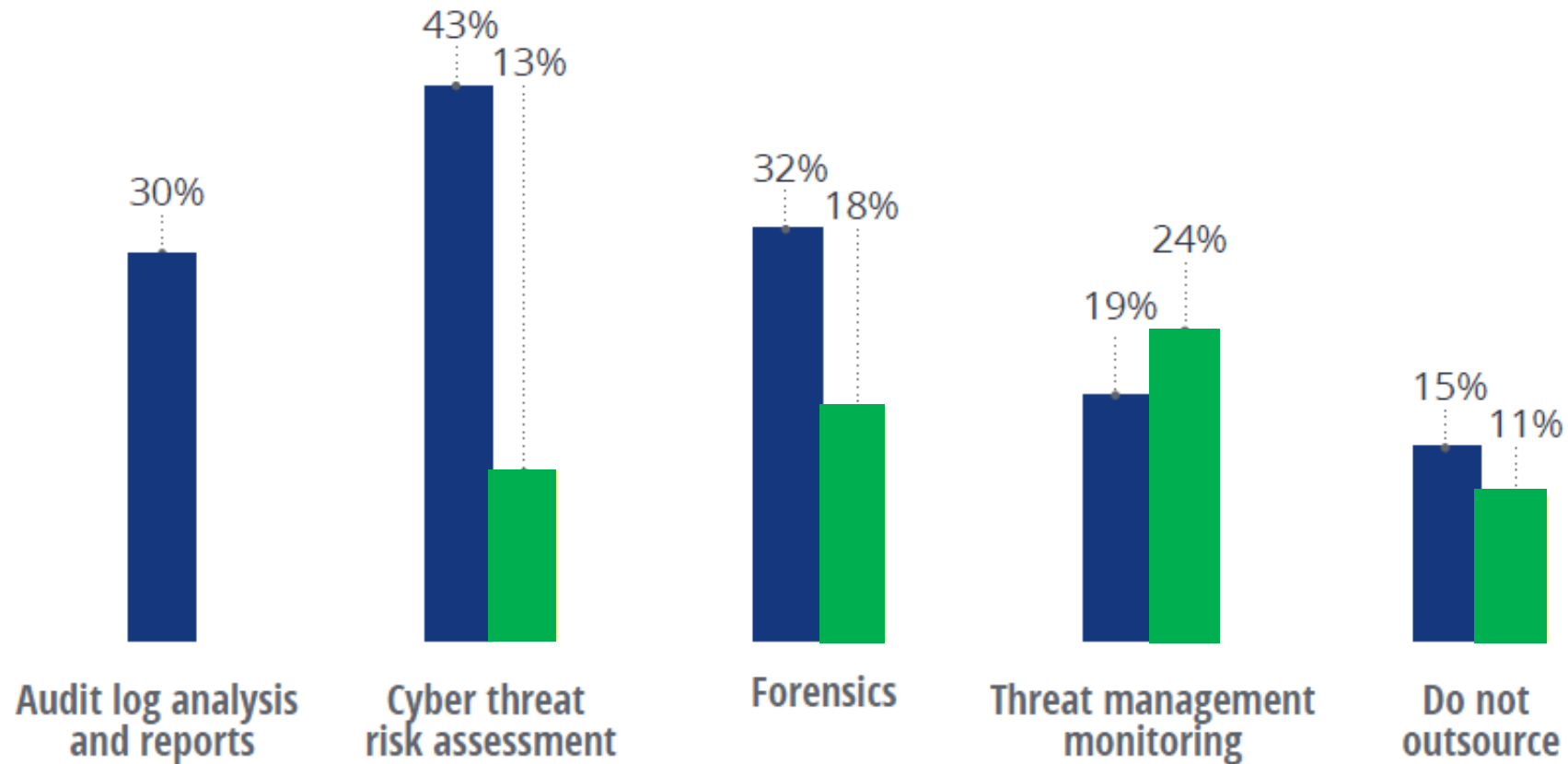
- 94%** State's salary rates and paygrade structures
- 51%** Workforce leaving for private sector careers
- 47%** Lack of qualified candidates due to demand from federal agencies and private sector
- 24%** Work location—lack of qualified cyber workforce in the state capital
- 18%** Outdated classifications and job descriptions for cybersecurity positions
- 12%** Lack of a defined career path and opportunities in cybersecurity
- 12%** Lengthy hiring process

Survey question: What are the top three human resource factors that negatively impact your ability to develop, support, and maintain the cybersecurity workforce within your state? (49 respondents)

# Talent crisis

While outsourcing has increased for certain functions, more than half of US states have yet to outsource many of them

■ 2018 ■ 2010



Survey question: Select the cybersecurity functions that your state outsources. (47 respondents)

# Bold Play#3: Team with the Private Sector and Higher Education



## TEAM WITH THE PRIVATE SECTOR AND HIGHER EDUCATION

CISOs should leverage public-private partnerships and collaborations with local colleges and universities to provide a pipeline of new talent, as well as consider outsourcing to private-sector firms.





# Montana's Story

---



# NICE Workforce Categories

---

Categories	Descriptions
Securely Provision (SP)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.
Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.



# The State of Montana and the NICE Framework

# The NICE Framework (NIST SP 800-181)

---

- Describes cybersecurity work and workers
- Establishes a common lexicon
- Sector and Industry agnostic
- Components:
  - Categories (7) – A high-level grouping of common cybersecurity functions.
  - Specialty Areas (33) – Distinct areas of cybersecurity work.
  - Work Roles (52) – The most detailed groupings cybersecurity work comprised of specific KSAs required to perform tasks in a work role.

# NICE Framework in the State of Montana

---

- The State of Montana uses the NICE Framework to:
  - Assess cybersecurity workforce
  - Assess cybersecurity program
  - Develop workforce (retention and) training plans
  - Develop workforce hiring plans

# Assess Cybersecurity Workforce

---

## **Step 1: Assess cybersecurity workforce**

- Evaluate NICE Work Roles performed by each worker
  - Which NICE Work Roles are currently performed?
  - Which NICE Work Roles are not currently performed?
  - Which NICE Work Roles do we need to fill?

# Assess Cybersecurity Program

---

## **Step 2: Assess cybersecurity program**

- Assign NICE Categories to each bureau based on step 1 results
- Evaluate NICE Specialty Areas assigned to each bureau
  - Which NICE Specialty Areas are complete?
  - Which NICE Specialty Areas are not complete?
  - Which NICE Specialty Areas do we need to complete?

# Develop Workforce Training Plans

---

## **Step 3: Develop workforce (retention and) training plans**

- Evaluate which needed-but-incomplete NICE Specialty Areas can be completed by existing workers based on step 2 results
  - Which workers are best positioned to complete the needed NICE Specialty Areas?
- Evaluate training for each worker based on step 1 results
  - What training is most appropriate for each worker to complete the needed NICE Specialty Areas?
- Provide appropriate training to each worker to complete each needed NICE Specialty Area



# Develop Workforce Hiring Plans

---

## Step 4: Develop workforce hiring plans

- Evaluate which needed-but-incomplete NICE Specialty Areas cannot be completed by existing workers based on step 2 results
- Create job descriptions for new workers based on needed-but-incomplete NICE Specialty Areas and on step 1 results
  - What Knowledge, Skills, Abilities do new workers need to complete the required Tasks?
- Hire appropriate new workers to complete each needed NICE Specialty Area

# How did Montana do it?

---

- Highlighted which functions in NICE appendix each existing staffer performs then did a SWOT and gap analysis to see what they were missing
- No in-state cyber pipeline, attracted out of state
- Compared national job descriptions and looked for unfilled jobs that matched
- Ranked positions on salary to see how to attract out of state employees
- Creating an apprentice program
- Creating an internship program

# How did Montana do it?

---

- Had off the record sessions with the legislative committee members, built relationships and established buy-in
- Received \$6.3 million, the money will be in the Montana cybersecurity budget permanently
- Showed the data, made it a process, and communicated the need
- Revised current team member salaries and used higher salaries for new positions
- Created flexible work schedules and encouraged training and certifications (and paid for them!)
- Emphasized state service and work life balance and provided relocation assistance

# Contact Information

---

**Meredith Ward**

Director, Policy & Research  
NASCIO

[mward@nascio.org](mailto:mward@nascio.org)



**Tara Mahoutchian**

Senior Manager, Human Capital  
Deloitte

[tmahoutchian@deloitte.com](mailto:tmahoutchian@deloitte.com)

**Deloitte.**

**Andy Hanks**

CISO,  
State of Montana  
[andrew.hanks@mt.gov](mailto:andrew.hanks@mt.gov)

