The Quest For

# Proactive Threat Hunting Capabilities

A new survey of financial, healthcare, energy, technology, transportation and government IT leaders highlights the need for a more proactive approach to cybersecurity.

Presented by cyberscoop

Underwritten by Raytheon

## In a new survey

**of IT leaders across America's top industries and government, CyberScoop and FedScoop identify:**

- The top cybersecurity concerns and strategies driving IT officials in the financial, healthcare, energy/utilities, technology and transportation sectors and in government
- How agile and proactive IT leaders say their organizations are in addressing emerging cybersecurity threats.
- The expanding importance of artificial intelligence in cybersecurity
- The key skills and characteristics industry and government executives are now looking for when hiring cybersecurity workers
- A sector-by-sector breakout of cybersecurity capabilities and network and endpoint visibility
- The importance of third-party specialists in helping industry and government detect and respond to emerging threats

CyberScoop and FedScoop conducted an online survey of pre-qualified executives in five leading industries and in federal and state government about their top concerns and practices surrounding cybersecurity. A total of 251 executives completed the survey in May 2018.

## Breakout by industry

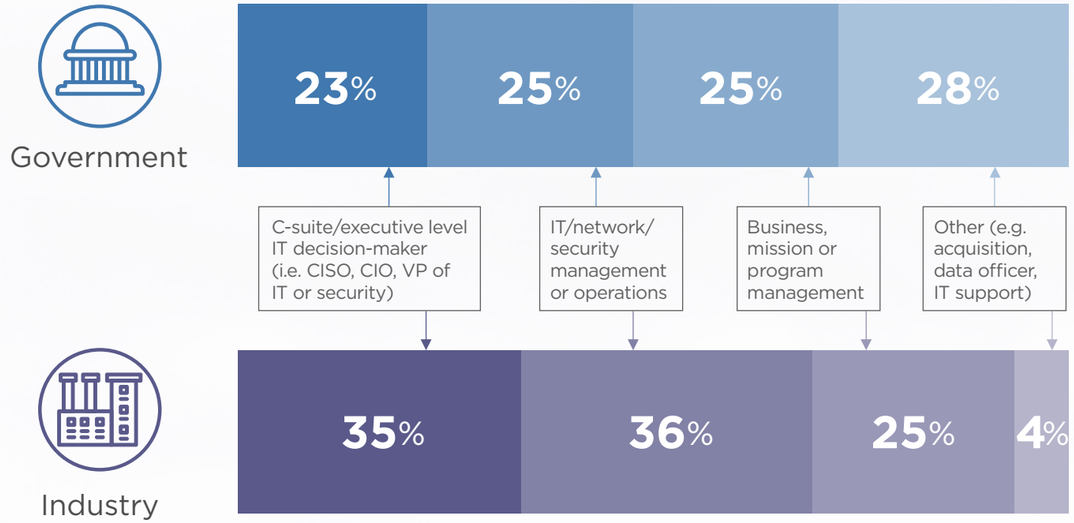
**69** Government

**182** Industry

- **Energy/Utilities Sector** — **15%**
- **Financial Sector** — **15%**
- **Healthcare Sector** — **15%**
- **Transportation Sector** — **15%**
- **Technology Sector** — **32%**
- **Services** — **7%**

** Percentages don't add to 100% due to rounding*

## Breakout by job title




## All respondents are involved in one or more areas of responsibility

- **58%** Identify the need for cybersecurity services, solutions or vendors
- **49%** Determine cybersecurity requirements, specifications, features, services or vendors
- **40%** Make the final decision regarding cybersecurity services, solutions or vendors
- **39%** Implement or manage cybersecurity solutions
- **31%** Allocate budget dollars for cybersecurity solutions
- **14%** Involved in IT, but not with cybersecurity

** Percentages exceed 100% due to multiple responsibilities*

## The state of cybersecurity agility and preparedness

- Among the top cybersecurity concerns of financial, healthcare, energy, technology, transportation and government IT executives:
  - 57% said, “Being able to detect/respond to threats quickly enough.”
  - 50% said, “Being able to adapt to changing cybersecurity threats.”
  - 41% said, “Attracting talent” and “Complying with security mandates.”

- 60% of government respondents rated their organization’s agility in proactive threat hunting as average or below average, compared to 34% of industry respondents.

- Artificial intelligence is being used for cybersecurity by 6 in 10 respondents at industry organizations, compared to 3 in 10 in government.

- 64% of industry IT executives say they are investing 10% or more of their 2018 cybersecurity budget on AI technology, compared to 34% in government.

- A breakout of the results by sector found financial and transportation organizations are doing a more effective job at preventing cybersecurity incidents, compared to healthcare, energy and technology organizations; government organizations are least effective.

- The need for skilled talent remains a critical challenge. But the greatest need now is for proactive, analyst-minded individuals who can think like a hacker, and individuals with threat hunting capabilities.

- Roughly half of respondents in every industry sector said their organization outsources 20% or more of their cybersecurity work; government and technology organizations outsource less often.

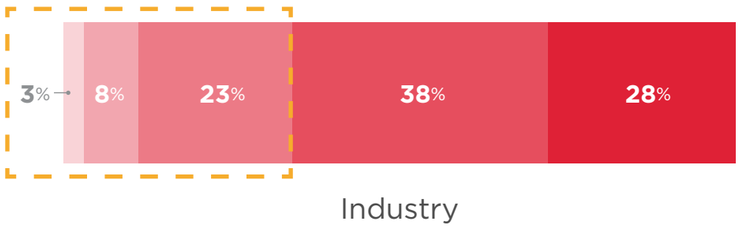
- Two-thirds or more of respondents agreed they could benefit from third-party assessments, roadmaps and process development.

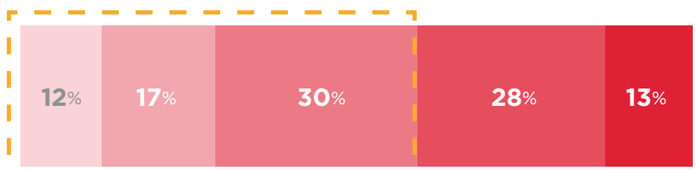
**6 in 10 government IT leaders** rated their organization's agility in proactive threat hunting as **average or below average**, compared to **3 in 10 industry respondents**.

**57% of government respondents** rated their organization's agility as **average or below average** in being able to adapt to changing threats, compared to **30% of industry respondents**.

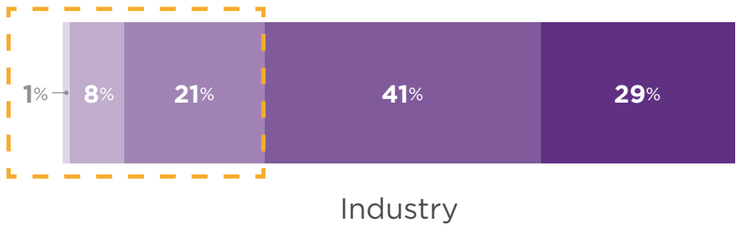
**78% of industry respondents** rated their organization's speed of response to emerging threats as **high to very high** in agility, compared to **61% of government respondents**.

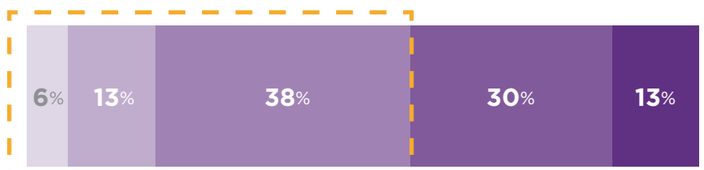
### Proactive threat hunting



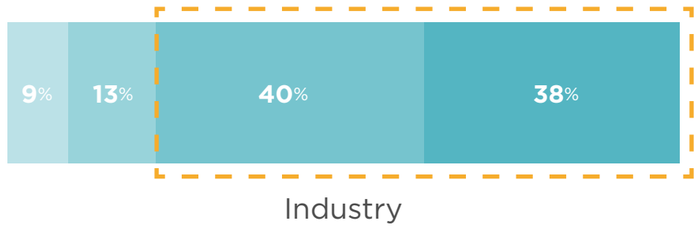



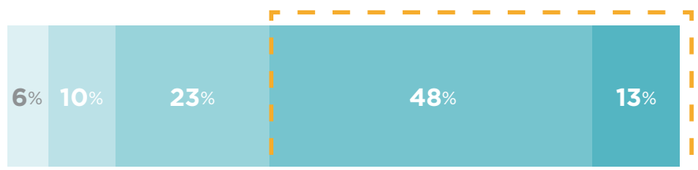

### Ability to adapt to changing threats




### Speed of response/response time



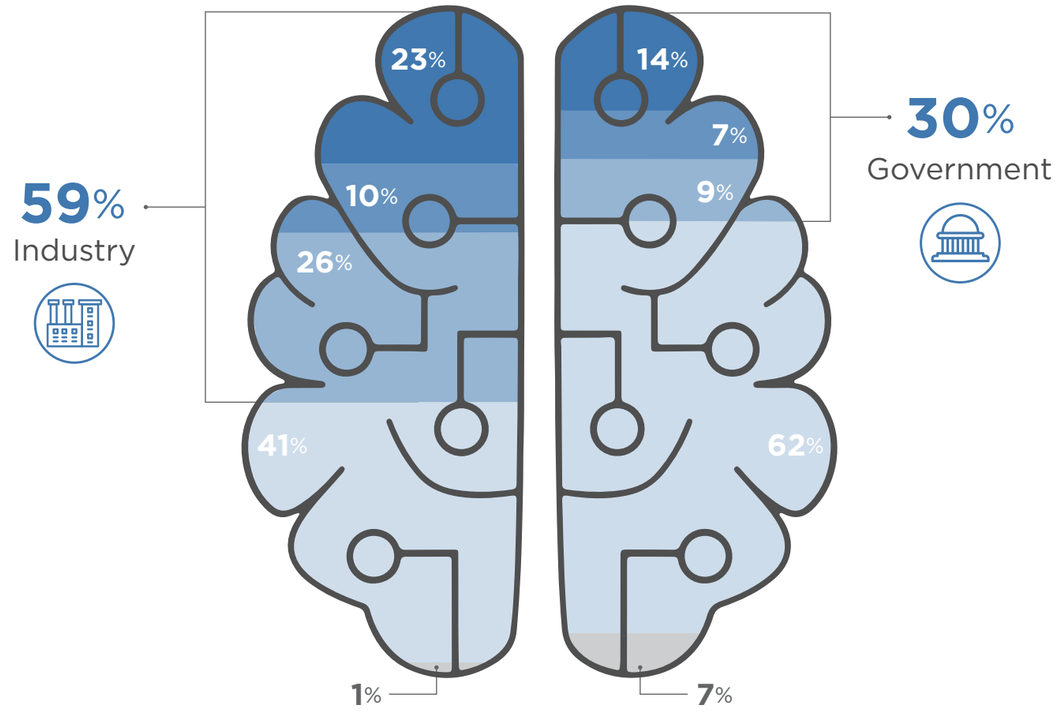





*Q: On a scale of 1 to 5, how agile is your organization when it comes to addressing emerging cybersecurity threats?*

**59% of industry respondents** say their organizations are using artificial intelligence to address cybersecurity, in contrast to **30% of government respondents**.

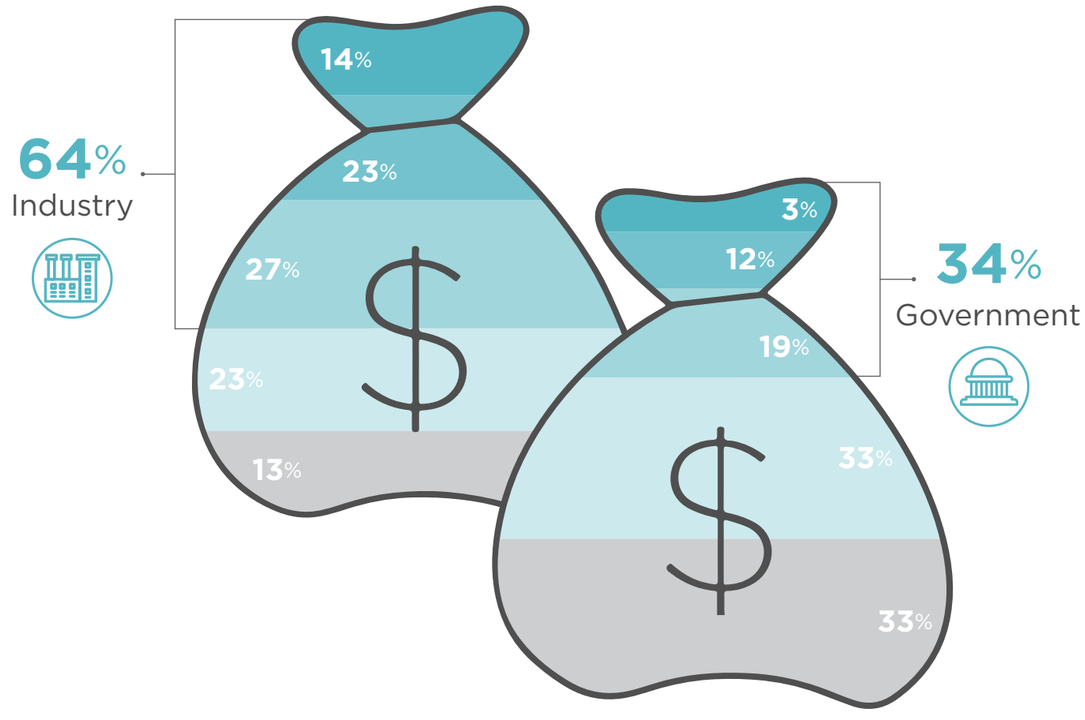
- Our AI is able to understand and adapt to changing advanced security threats
- We use AI to thwart attackers
- We use AI to identify threats
- We are not using artificial intelligence
- Not sure




*Q: How is your organization using artificial intelligence (AI) in cybersecurity?*

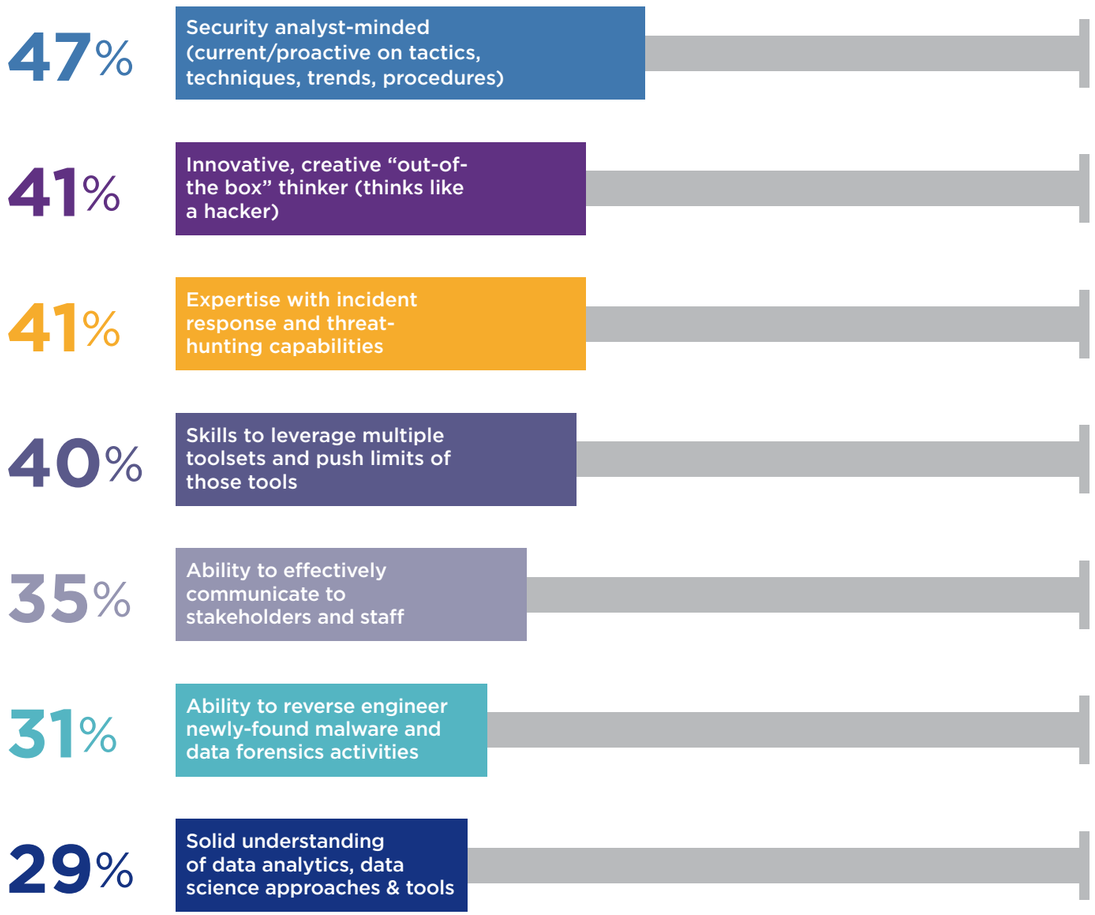
**64% of industry respondents** say their organizations are investing 10% or more of their 2018 cybersecurity budget on AI technology, compared to **34% of government respondents**.

- 30% or more of cybersecurity budget invested in AI
- 20–29%
- 10–19%
- 0–9%
- Not sure



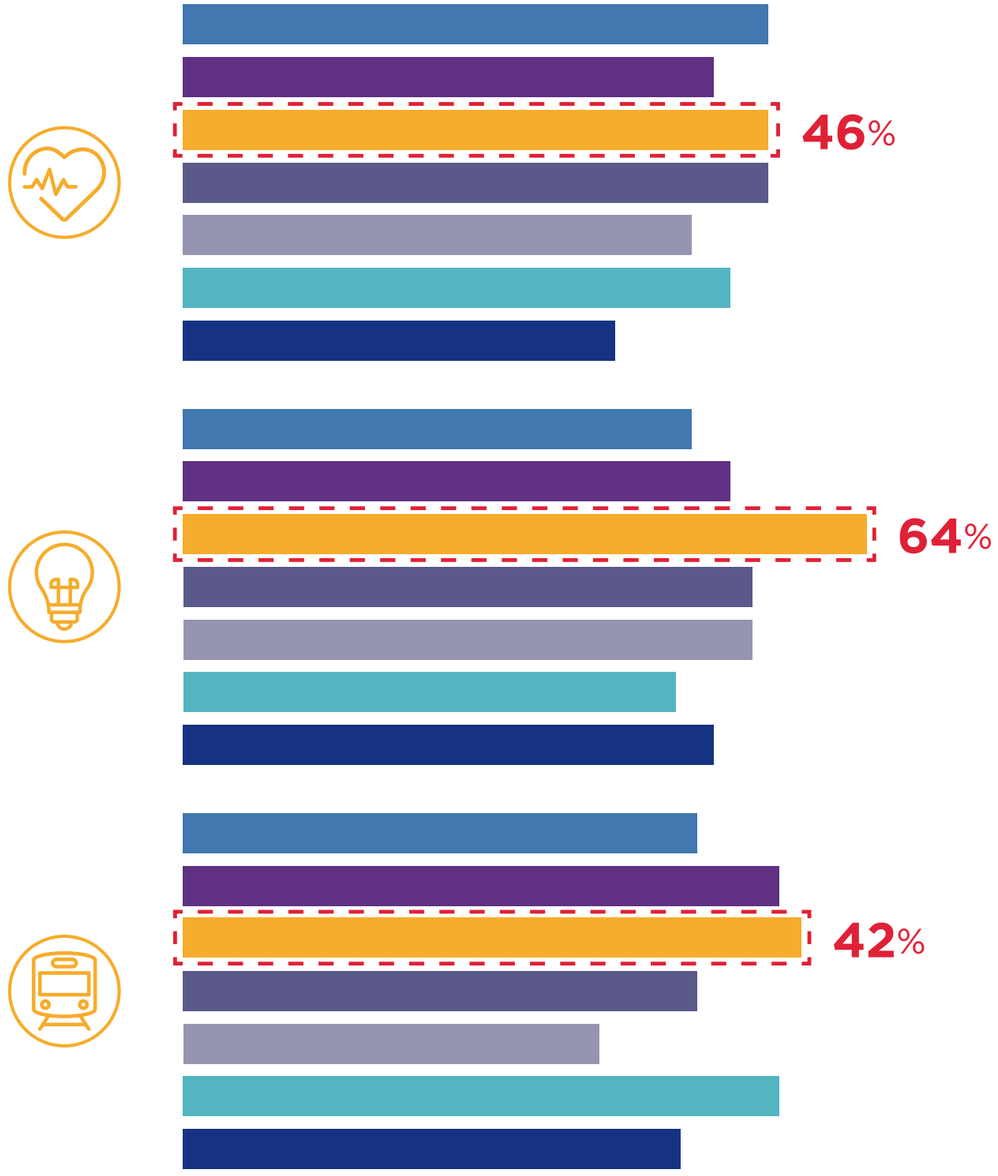

*Q: About what percent of your cybersecurity budget in 2018 will go to artificial intelligence technology?*

The need for skilled talent remains a critical challenge. But IT executives said their **greatest need** now is for **proactive, analyst-minded** individuals who can **think like a hacker**.




** Percentages exceed 100% due to multiple responses*

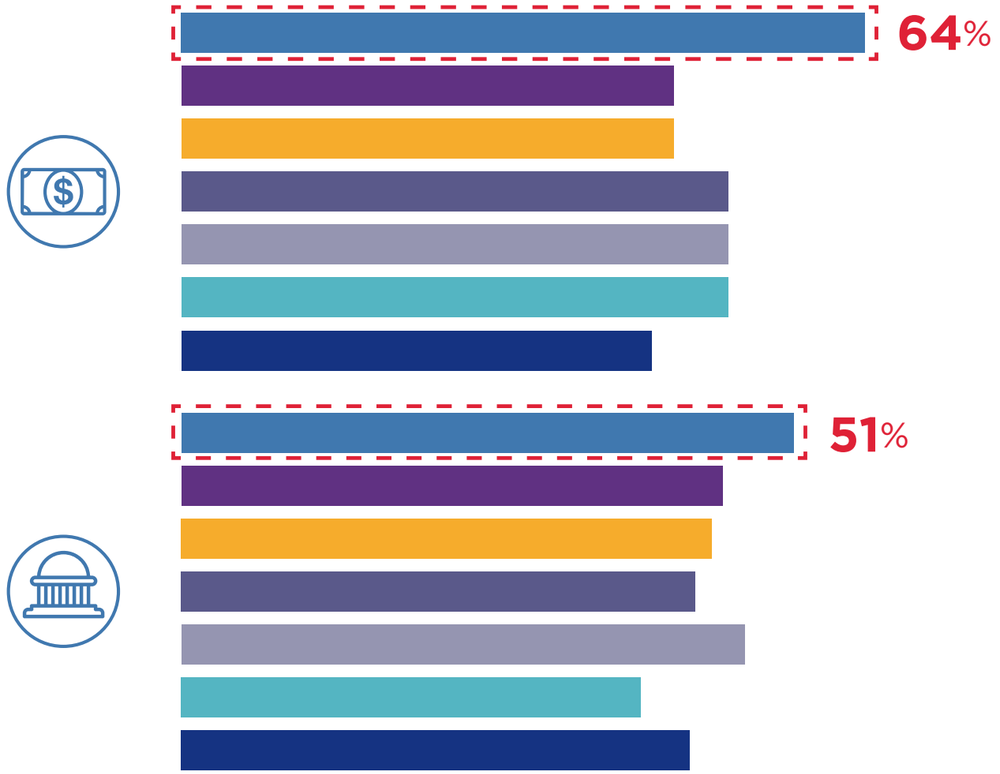
**Health**, **energy** and **transportation** leaders gave top priority to **experts with incident response and threat hunting capabilities**.



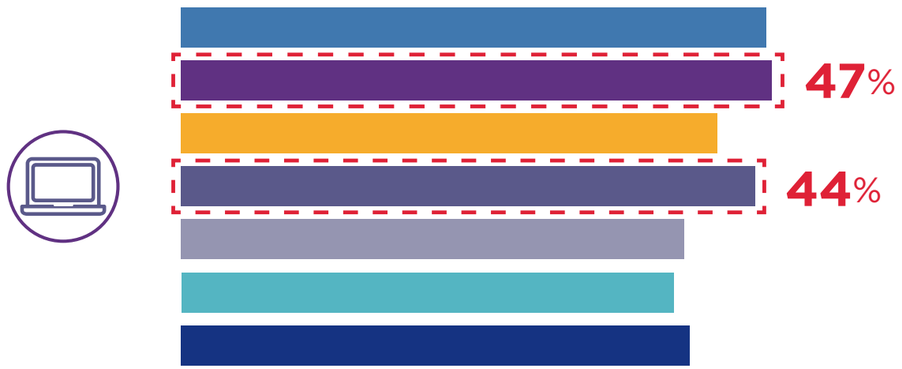

*Q: What are the key skills and characteristics you look for when hiring cybersecurity workers? (Select up to three)*

- Security analyst-minded (current/proactive on tactics, techniques, trends, procedures)
- Innovative, creative “out-of-the box” thinker (thinks like a hacker)
- Expertise with incident response and threat-hunting capabilities
- Skills to leverage multiple toolsets and push limits of those tools
- Ability to effectively communicate to stakeholders and staff
- Ability to reverse engineer newly-found malware and data forensics activities
- Solid understanding of data analytics, data science approaches and tools

**Financial** and **government** respondents said their greatest need was for **security analyst-minded individuals**.



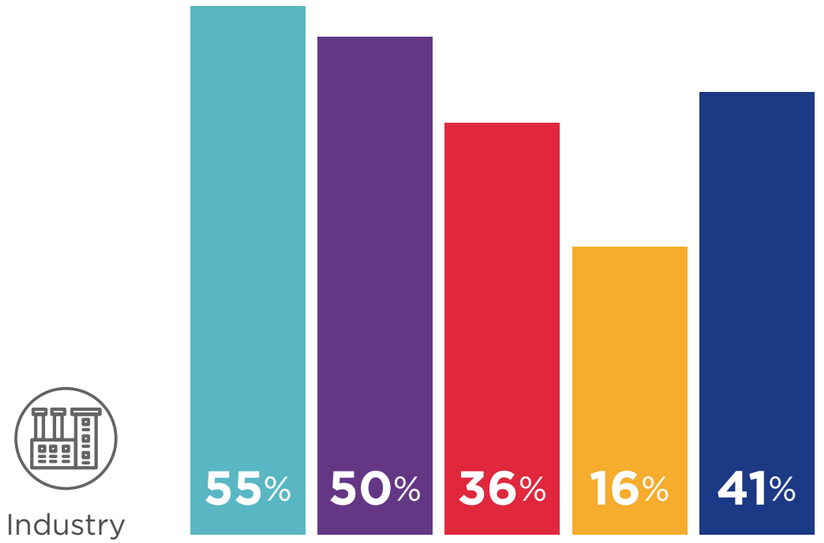

**Technology** sector leaders want individuals who can **think like a hacker** and **leverage multiple toolsets**.

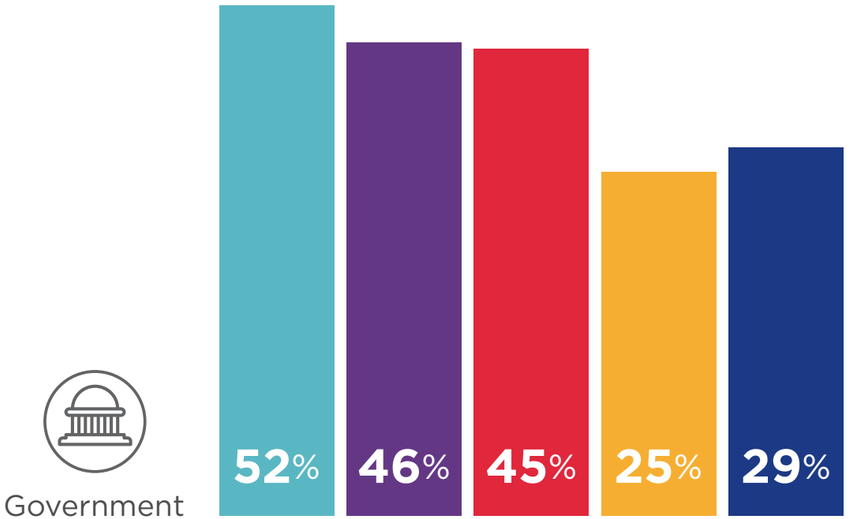


Overall, leaders in industry and government said their top staffing concerns centered around **finding/retaining enough qualified workers** and the **lack of cybersecurity staff knowledge/expertise**.

The **lack of proactive threat hunting skills on staff** was of next greatest concern for industry. For government, it was **keeping up with the speed of security changes/threats**.

- Finding and retaining enough qualified workers
- Lack of cybersecurity knowledge and expertise among my staff
- My staff isn't able to keep up with the speed of changing security/technology threats
- My staff is not collaborative enough
- Lack of proactive threat hunting among my staff



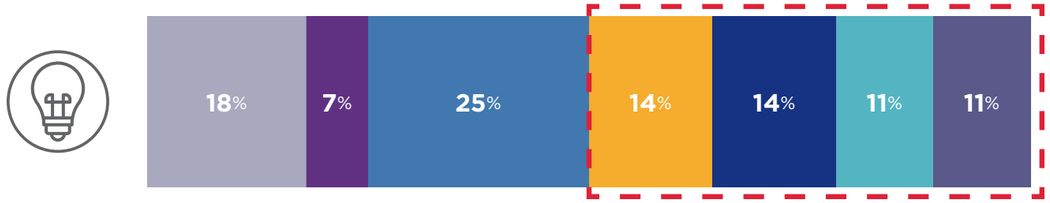



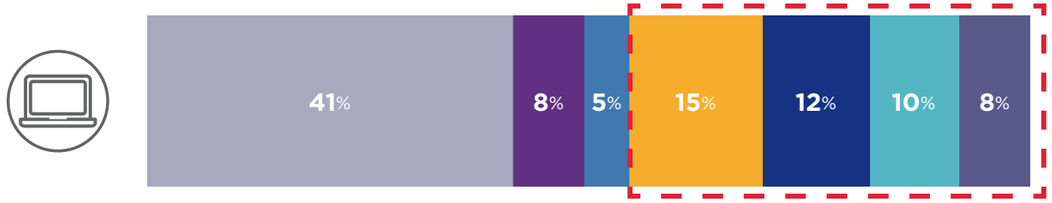

*Q: Which of the following cybersecurity staffing issues are top concerns for your organization? (Select up to three)*

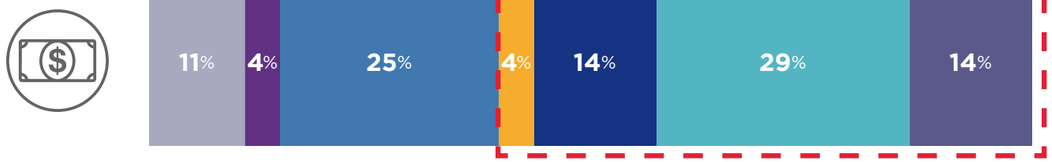
**Roughly half** of respondents in **every industry sector** report **outsourcing more than 20% of their cybersecurity work**.

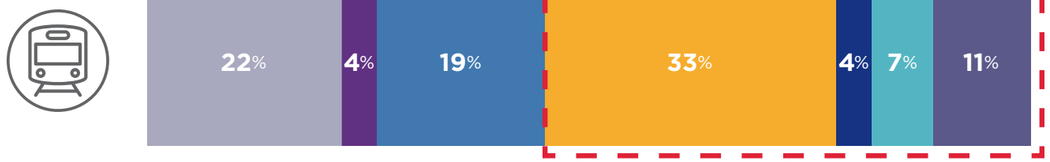
A significant portion of **technology** and **government** respondents say they **do not outsource their cybersecurity work**.

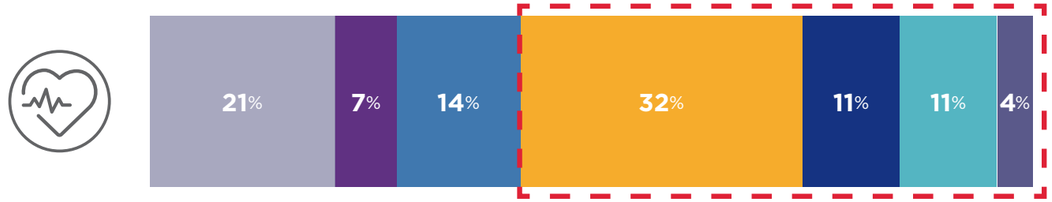
- We do not outsource
- 1–10%
- 11–20%
- 21–30%
- 31–40%
- 41–50%
- More than 50%



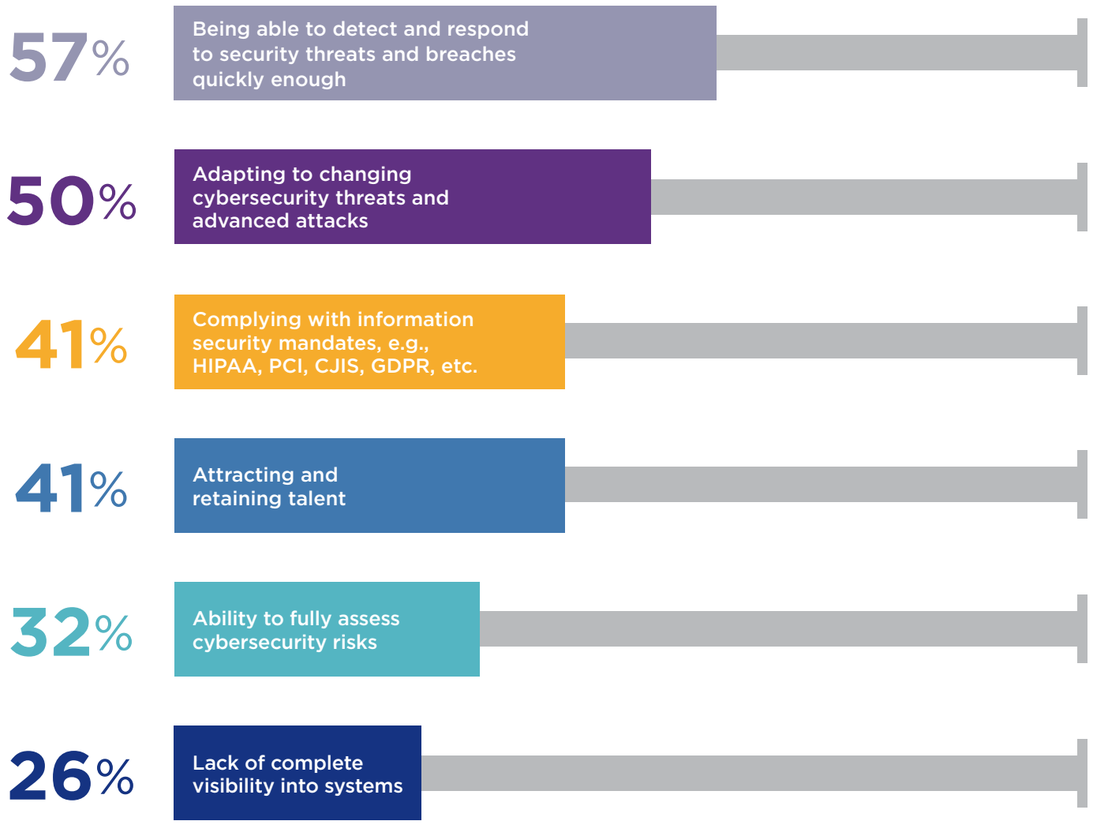





*Q: What percent of your organization's cybersecurity work do you outsource?*

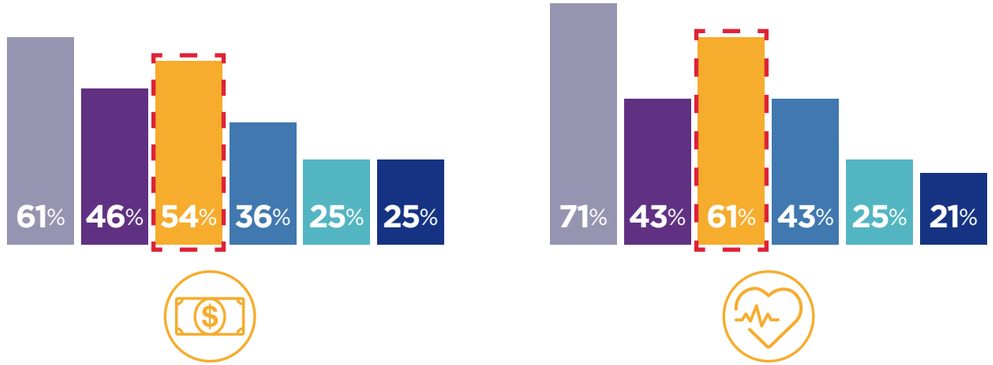
**Being able to detect and respond to security threats and breaches quickly enough** was the top concern among industry and government respondents.



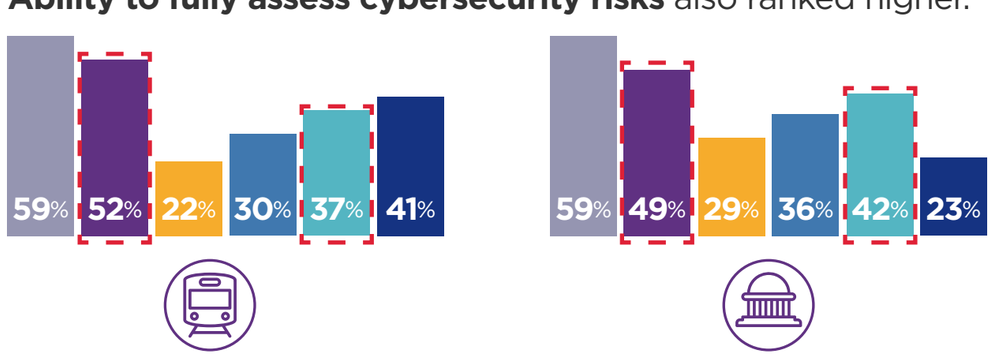

** Percentages exceed 100% due to multiple responses*

*Q: Which of the following top cybersecurity concerns keep you up at night? (Select up to three)*

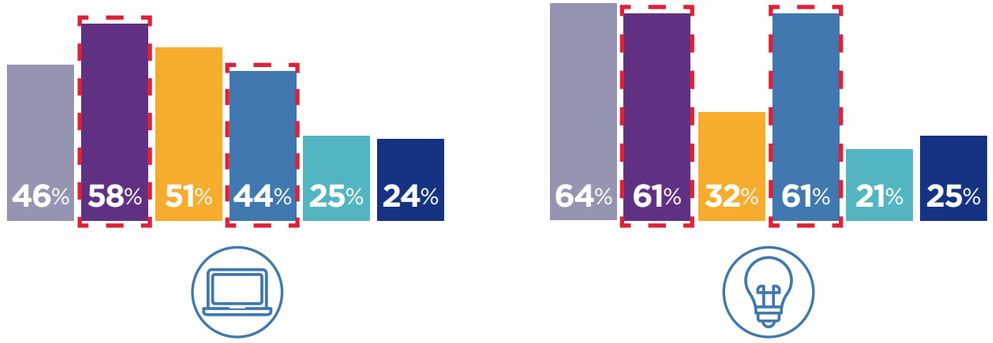
**Complying with information security mandates** ranked #2 for financial and healthcare sector respondents.



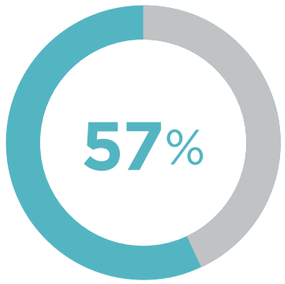

**Adapting to changing security threats and advanced attacks** ranked #2 for transportation and government respondents. **Ability to fully assess cybersecurity risks** also ranked higher.



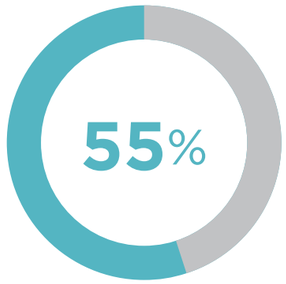

Technology and energy respondents tended to rank **adapting to changing threats** and the need for **attracting and retaining talent** higher.



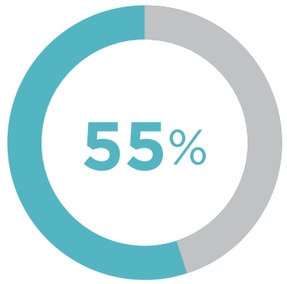
Industry and government executives said their organizations are taking multiple proactive steps to make it harder for attackers, including:



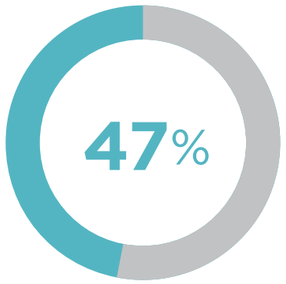

**E-mail protection tools/tactics, i.e. DMARC**



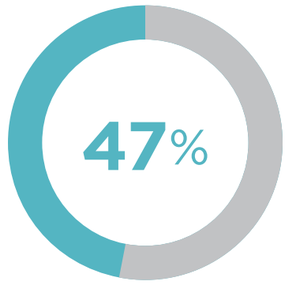

**Identity management solutions**



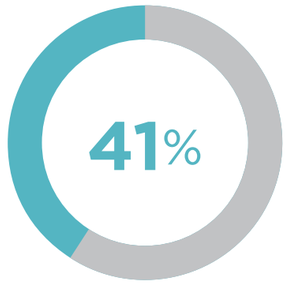

**Apply security policies for firewall, proxies, user access**



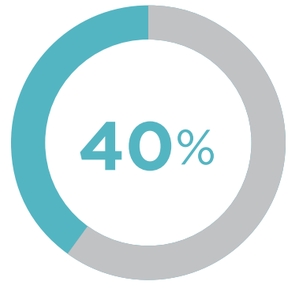

**Periodic vulnerability/ security assessments**




**Endpoint management solutions**




**Tools that protect, configure, isolate wireless networks**

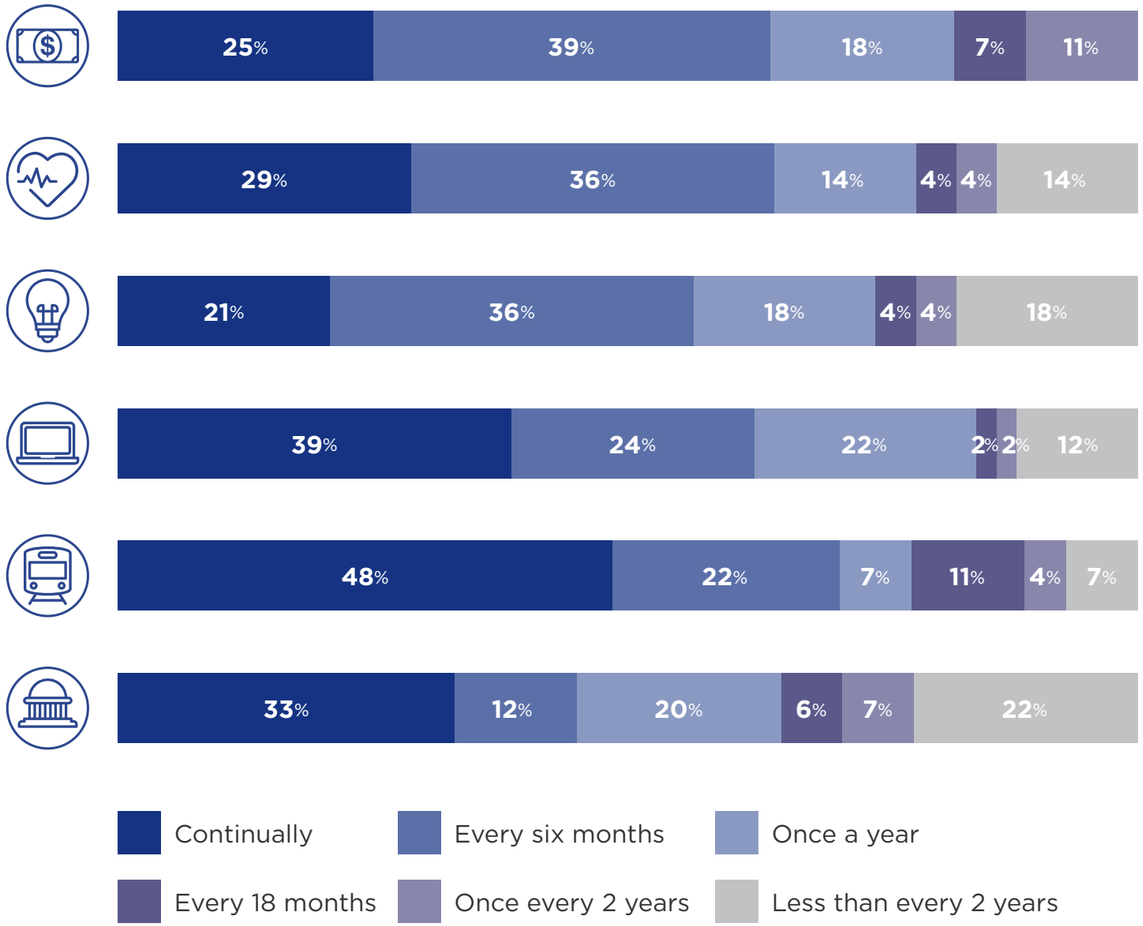



**DDos protection, application whitelisting, secure enclaves**

*Q: Which of the following proactive steps is your organization taking to make it harder for attackers? (Select all that apply)*

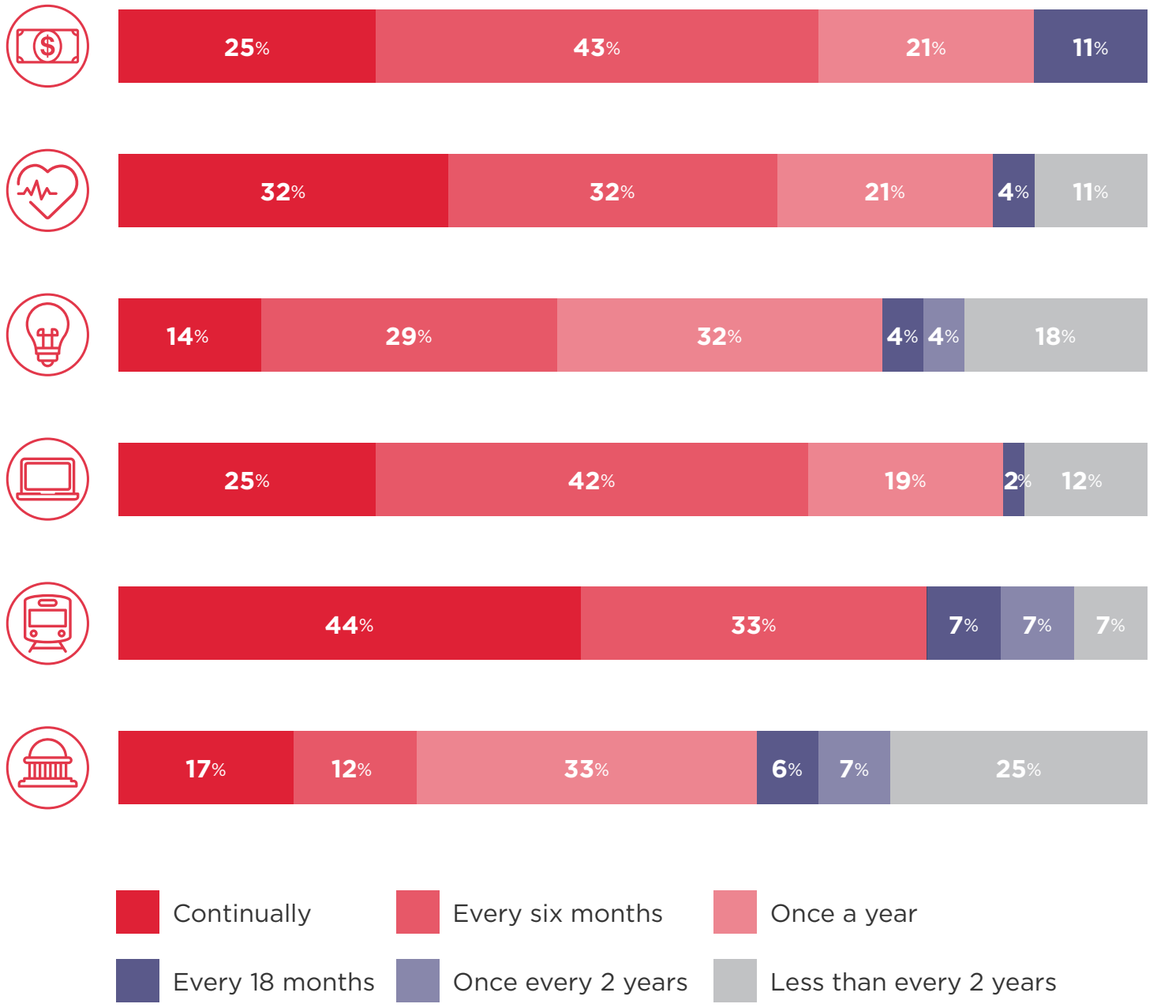
Roughly **two-thirds of industry respondents** in every sector say their organizations perform "blue team" vulnerability assessments at least **every 6 months**, **compared to 45% of government respondents**.

Nearly **half of transportation sector respondents** report their organizations perform blue team assessments **continually**.




*Q: How often do you conduct Blue Team vulnerability assessments?*

Roughly **2 in 3 transportation**, **financial** and **technology sector respondents** say their organizations perform “red team” penetration tests at least **every 6 months**, compared to **fewer than 3 in 10 government respondents**.




*Q: How often do you conduct Red Team penetration tests?*

## Detection

**89% of financial respondents**, **83% in technology** and about **80% in healthcare** and **transportation** rated their organizations as **highly or completely effective** at **detecting** cybersecurity incidents.

**40% of government respondents** and **36% in energy** rated their organization's ability to **detect** cybersecurity incidents **average to below average**.

## Response

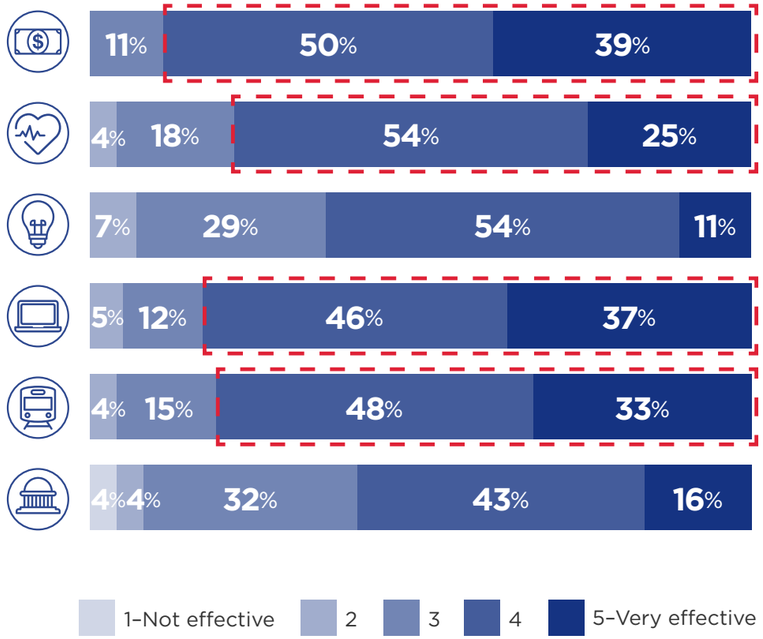
**92% of financial respondents**, **85% in transportation** and **76% in technology** ranked their organizations as **highly-to-completely effective** in **responsiveness** to cybersecurity incidents.

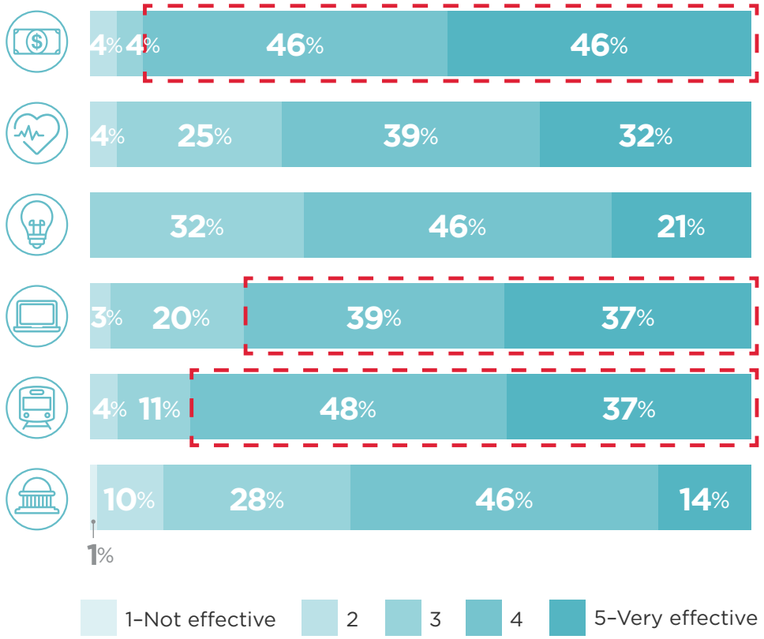
**Government, energy and healthcare respondents** gave their organizations **lower marks** for **responsiveness** effectiveness to cybersecurity incidents.

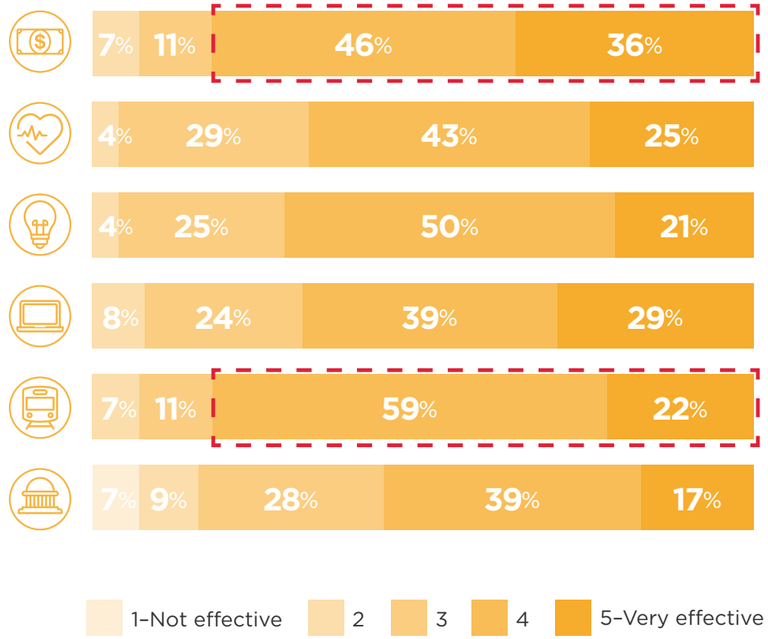
## Prevention

**Financial and transportation respondents** ranked their organizations **most effective** in **preventing** cybersecurity incidents.

**Government respondents** ranked their organizations **less effective** in **preventing** cybersecurity incidents.



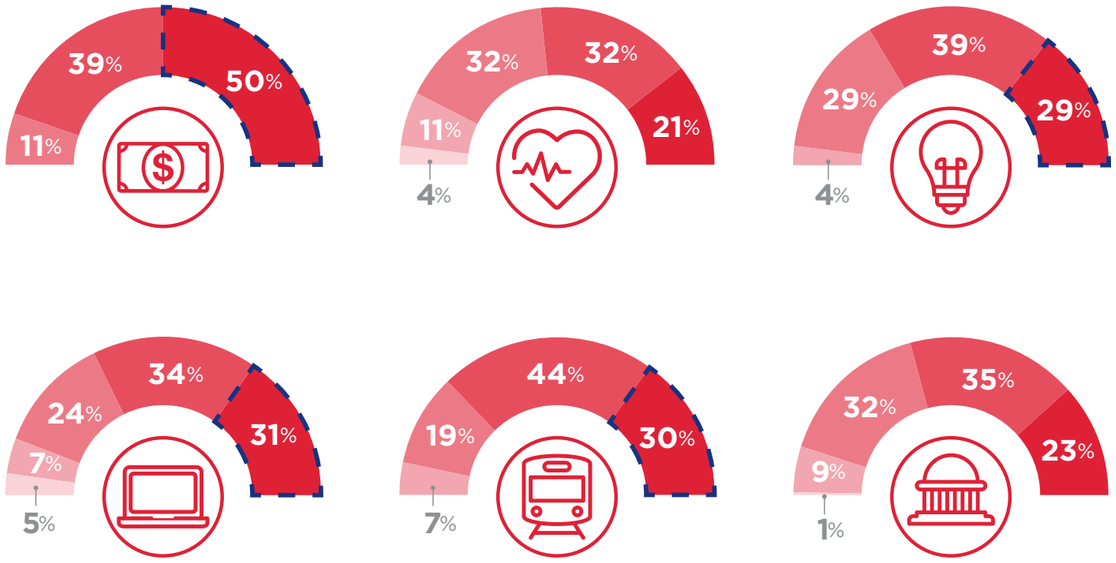




*On a scale of 1-5, how would you rate your organization's ability to detect, respond to, and prevent cybersecurity incidents?*

**Half** of **financial respondents** said their organizations have complete visibility of endpoint/mobile device security, compared to only **3 in 10** respondents in **energy**, **technology** and **transportation** — and slightly more than **2 in 10** in **healthcare** and **government**.

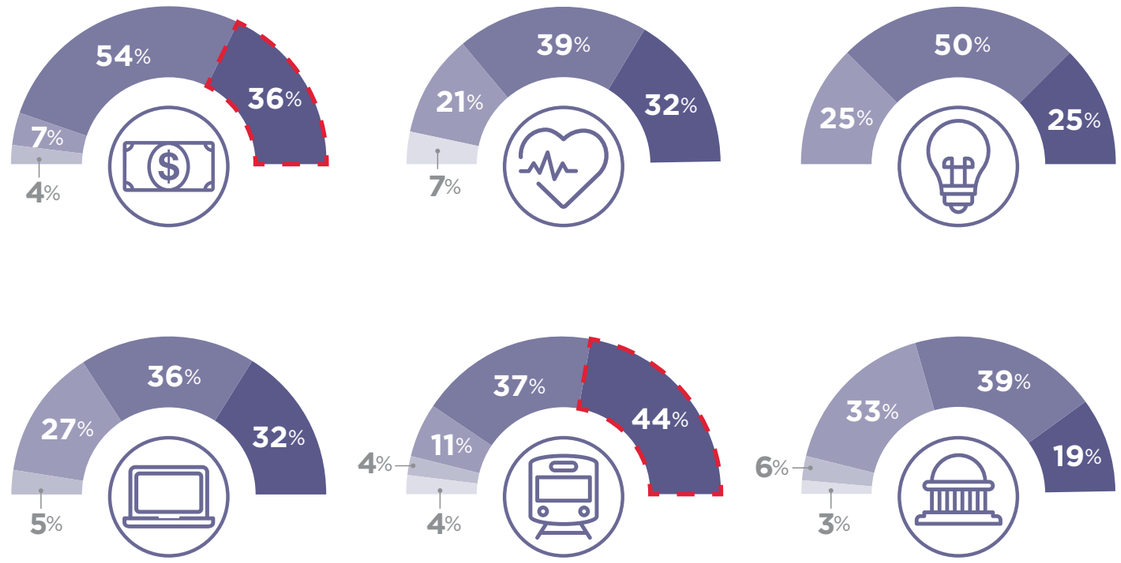
Respondents in **financial** and **transportation** organizations reported the **most complete security visibility** of their network infrastructure. **Government** respondents reported the **least visibility**.

## Endpoint/Mobile Devices




*On a scale of 1 to 5, how complete is your organization's security visibility of endpoint/mobile device security?*

## Network Infrastructure

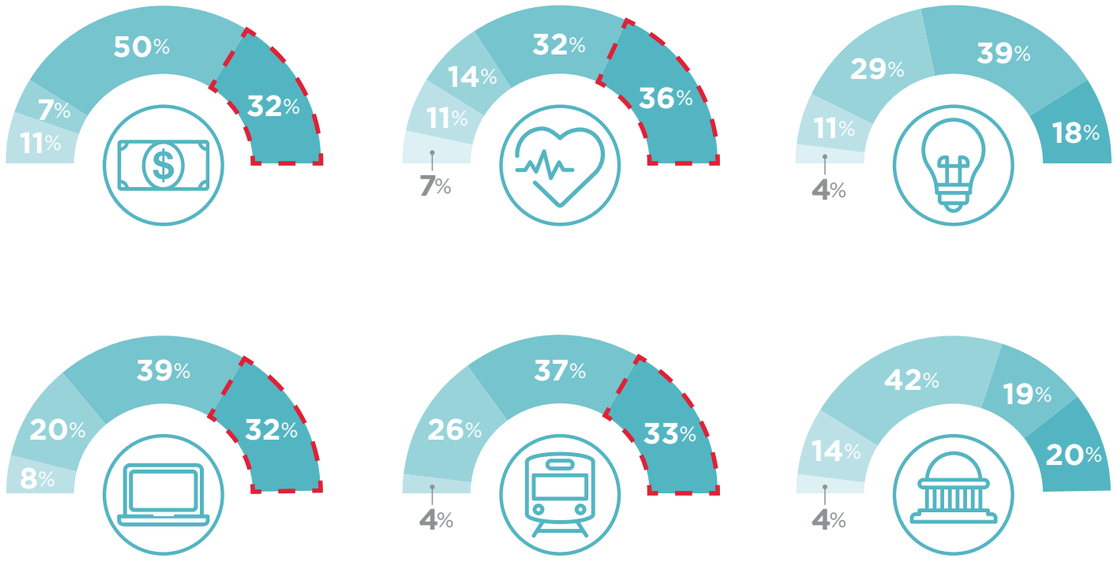



*Q: On a scale of 1 to 5, how complete is your organization's security visibility of network infrastructure?*

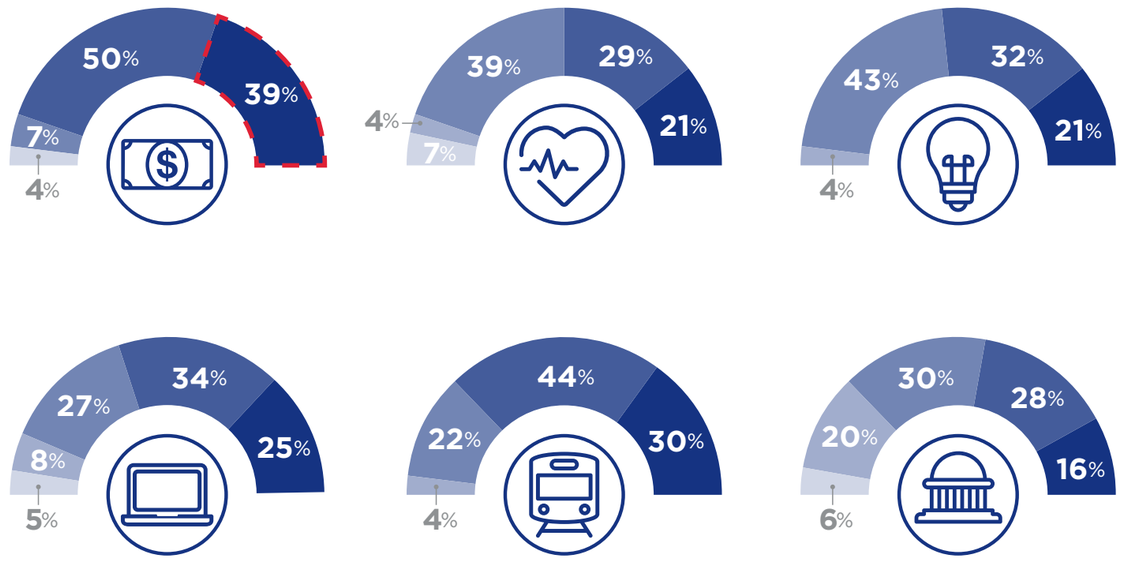
About **1 in 3 financial**, **healthcare**, **technology** and **transportation respondents** said they have **complete security visibility** of cloud applications and platforms, compared to **2 in 10** in **government** and **energy** sectors.

The **financial sector** is **further along** than other sectors in having **complete visibility** of systems and devices operated by third-party contractors who connect to their network.

## Cloud Applications & Platforms




## Third-party Systems & Devices

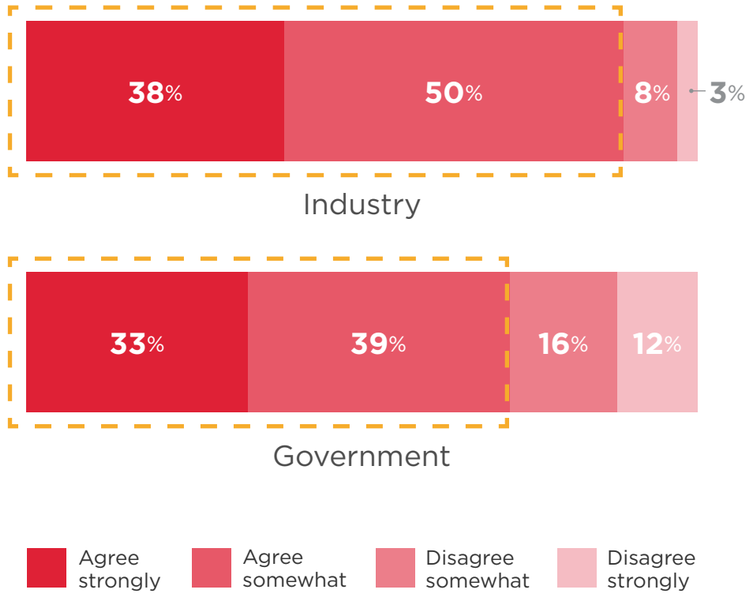



*Q: On a scale of 1 to 5, how complete is your organization's security visibility of cloud applications, including public, private or hybrid cloud services?*

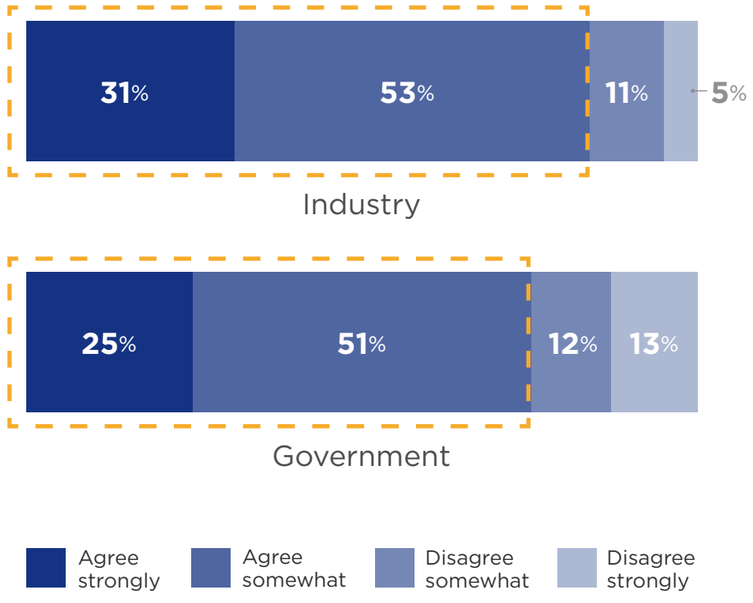
*Q: On a scale of 1 to 5, how complete is your organization's security visibility of systems and devices operated by third party contractors, which connect to our networks?*

Government respondents, and industry executives even more so, agree their organizations could benefit from third-party help, including:

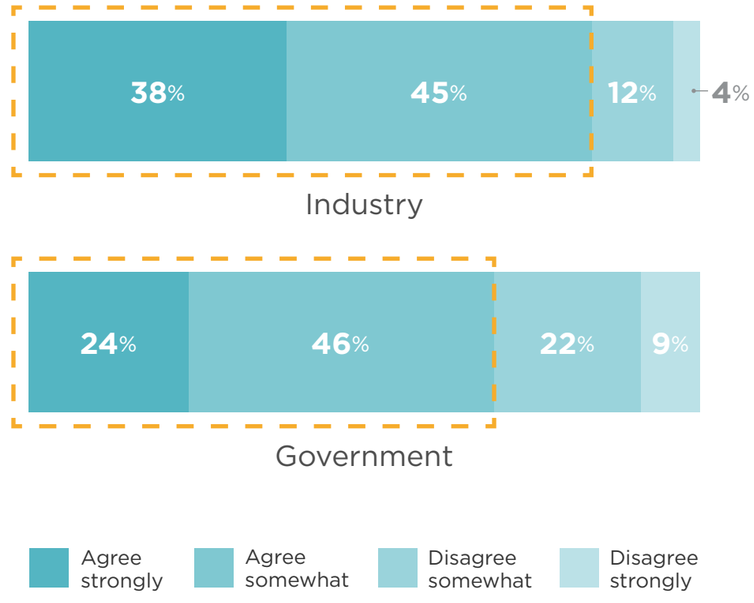
**Third-party assessments** to improve cybersecurity posture, capabilities and prevention methods.

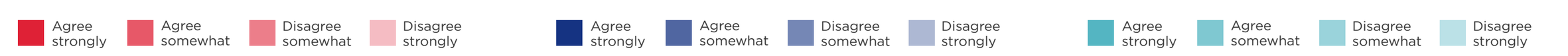



**A third-party roadmap** to improve visibility, detection capabilities and incident response.



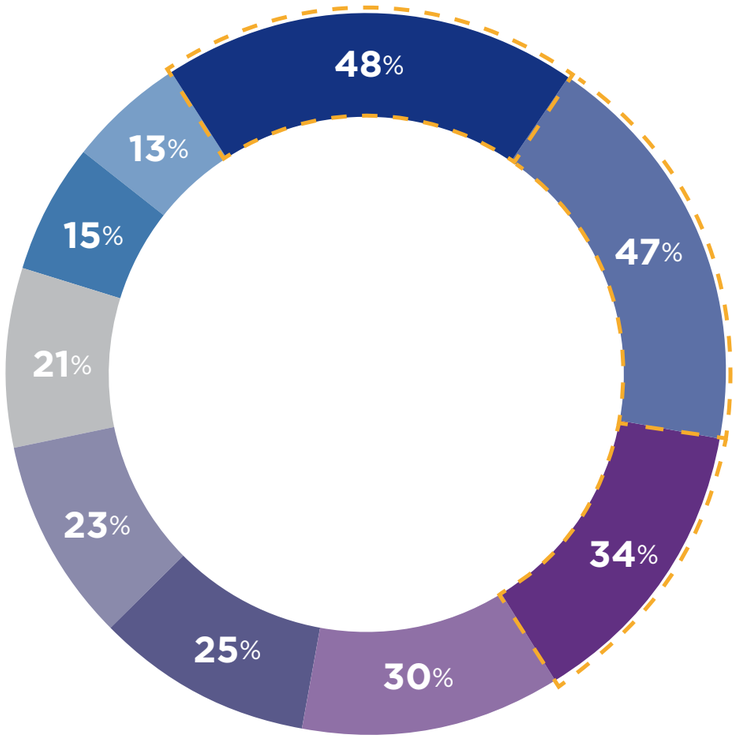

**Third-party development** of custom methods (i.e. rules, dashboards and behavioral) to improve detection of security threats.




*Q: To what extent do you agree or disagree my organization could benefit from...*

Respondents across all sectors said the top factors in choosing a security services provider was: **24/7/365 monitoring and detection**, **cost/price**, and **proactive threat hunting capabilities**.




- 24/7/365 ongoing monitoring and detection requirements
- Cost/price
- Proactive threat hunting capabilities
- Compliance (either not enough or disparate mandates)
- Lack of in-house talent
- Experience using multiple toolsets
- Project management
- Use of proprietary tools and methods
- We've had a serious security breach and need help right away

*Q: Which of the following are the top drivers when choosing an outsourced managed security services provider? (Select up to three)*

**Use of proprietary tools and methods** and **needing immediate help due to a security breach** were rated low in terms of driving factors when choosing to use third-party support.

1 IT leaders in financial and transportation sectors tend to be further along in preventing cybersecurity incidents, compared to those in the healthcare, energy/utilities and technology sectors, while those in government rated their organizations the least effective in the survey.

2 Industry organizations are outpacing government in their agility to use proactive threat hunting practices to address emerging cybersecurity threats.

3 Industry and government organizations alike are putting greater emphasis on looking for analyst-minded individuals who can think like a hacker and proactively hunt for threats.

4 Artificial intelligence is emerging as a key component to address cybersecurity, with nearly 2 in 3 industry executives reporting their organizations are investing 10% or more of their 2018 cybersecurity budget on AI technology.

5 Industry and government IT leaders also say being able to detect and respond to threats quickly enough and adapt to the changing cybersecurity landscape remain their top concerns.

6 Roughly half of respondents in every industry sector said their organization outsources 20% or more of their cybersecurity work. Two-thirds or more agreed they could benefit from third-party assessments, roadmaps and process development.

## About

**CyberScoop** is the leading media brand in the cybersecurity market. With more than 350,000 unique monthly visitors and 240,000 daily newsletter subscribers, CyberScoop reports on news and events impacting technology and security. CyberScoop reaches top cybersecurity leaders both online and in-person through our website, newsletter, events, radio and TV to engage a highly targeted audience of cybersecurity decision makers and influencers.

**FedScoop** is the leading tech media brand in the federal government market. With more than 210,000 unique monthly visitors and 120,000 daily newsletter subscribers, FedScoop gathers top leaders from the White House, federal agencies, academia and the tech industry to discuss ways technology can improve government and identify ways to achieve common goals. With our website, newsletter and events, we've become the community's go-to platform for education and collaboration.

## Contact

**Wyatt Kash**
Sr. Vice President, Content Strategy | Scoop News Group
Wyatt.Kash@FedScoop.com | 202.887.8001

Presented by cyberscoop

Underwritten by Raytheon