The Harris Poll

Harris Insights & Analytics, A Stagwell LLC Company

Public Sector Security Research

IBM-Harris Poll Survey 2020

IBM Security

Introduction

Table of Contents

Background & Objectives

The 2020 Public Sector Security Survey was conducted by The Harris Poll on behalf of IBM.

Key objectives for the research are to gain better understanding of public sector employees' awareness, knowledge, attitudes, and perceptions of cybersecurity threats. Specifically to:

- ✓ Identify the importance cities are putting on ransomware (e.g., prevention, preparedness, investment, etc.)
- ✓ Understand the resources public sector employees are being provided with (e.g., experts, training, tools, etc.)
- ✓ Gauge the progress, if any, that is being made to aid the situation
- ✓ Identify the biggest security weaknesses based on employee experiences
- ✓ Secure insights to gauge the public sector's overall outlook on this issue as we move into the new year

Research Method

Mode:
Online survey

Length:
12 minutes

Qualification Criteria:
- US residents
- State/local government employee
- Ages 18+

Weighting:
Data weighted to ensure results are projectable to appropriate U.S. populations

	All Employees In Public Sector	IT/Security	Emergency	Education
Sample Size:	*n=202*	*n=102*	*n=186*	*n=200*
Functional Role:	*All public sector departments*	*IT and related activities (computer programming, technical support, information services, security, etc.)*	*Public Safety (emergency management, emergency medical services, law enforcement, fire services)*	*Public Education (administrator, teacher K-12, higher education, teacher assistant, librarian, etc.)*
Field Dates:	January 16 – February 3, 2020			

Method Statement *(to be included in all press materials):*

This survey was conducted online by The Harris Poll on behalf of IBM among 690 employees who work for state or local government organizations in the United States. The survey was conducted January 16 through February 3, 2020 among adults 18+, employed full time or part time by local or state government. Four groups were captured in this survey:

1. Local and state employees (working across all public sectors)
2. Local and state employees in IT & related activities
3. Local and state employees in public safety/emergency response
4. Local and state employees in public education

Each group was weighted to their respective population by education, age, gender, race, Hispanic ethnicity, US region, household income, full-time/part-time employment status and local/state level to population benchmarks from the March 2019 Current Population Survey (CPS), conducted by the US Census Bureau. For all groups, propensity score weighting was also used to adjust for respondents' propensity to be online.

Report Notes

Throughout this report:

- ✓ In tables and charts, percentages may not add up to 100% due to weighting, computer rounding, and/or the acceptance of multiple responses.
- ✓ Unless otherwise noted, results for all 4 audiences are displayed side by side as follows:
  - ✓ **The audience which encompasses all roles and functions of state and local employees is being referred to as the "All Employees" audience.**
  - ✓ **The specialized state and local employees are being referred to by their key critical functions (IT/Security, Emergency, Education).**
- ✓ Colors and icons differentiate which audience is being represented within detailed findings slides:

- ✓ Where appropriate, statistically significant differences (at the 95% confidence level) between the audiences are noted with accompanying letters - a, b, c, and d.
  - ✓ For example, if the All Employees % is significantly higher than the Emergency %, the letter (c) will be placed next to the percentage for the All Employees audience.
  - ✓ A legend in the top right corner of each slide reminds the reader of the letter assignments.

All Employees (a)	Emergency (c)
IT (b)	Education (d)

Key Take-Aways

IN SUMMARY

Key Take-Aways

The threats posed by Ransomware and Cyberattacks have not gone unnoticed by government employees. The study found that 73% of government employees are concerned about impending ransomware threats to cities across the United States. Among "All Employees":

- ✓ One in two expect attacks in their community to rise in the next year.
- ✓ Six in ten can even imagine their own workplace being a victim of a cyberattack.
- ✓ A sixth has experienced a Ransomware attack firsthand.

Not surprisingly, there is also widespread concern about these attacks. In fact, over 50% of government employees express more concern about cyberattacks than any other threat, including the threat of natural disasters and terrorist attacks.

- ✓ 50% or more of "All Employees" feel that all systems measured (slightly less for Parks and Recreation) are at least somewhat vulnerable to cyberattacks.
- ✓ Most vulnerable in their minds are systems linked to Administrative Offices, Utilities and the Board Of Elections – as noted by two thirds or more of "All Employees."
  - ✓ Overall, 63% of these government employees are specifically concerned about the 2020 elections being disrupted.

Despite their recognition of the threats, government employees are also optimistic (and perhaps overly confident) about their employers' ability to overcome cyberattacks. Over half are confident that their employer could manage the consequences of an attack.

- ✓ In addition, among "All Employees":
  - ✓ 66% feel that their employer is prepared (at least somewhat) to deal with the threats to their services.
  - ✓ 74% are also confident in their own ability to recognize and prevent an attack.

IN SUMMARY

Key Take-Aways

Results suggest that employers may need to offer additional training and support. While three-quarters of "All Employees" have received at least some form of basic cybersecurity training – only 54% would agree that they received adequate training on how to respond to an attack.

- ✓ In addition, despite some reported improvement over last year, across sectors…
  - ✓ At least 30% disagree that their employer is investing enough in prevention.
  - ✓ 29% or more don't feel that their employer is taking the threat of cyberattack seriously enough.
  - ✓ Half or more have not seen any change in preparedness by their employer.
  - ✓ Two-fifths or more have also not seen any changes in the budgets and resources being dedicated to managing the threat of cyberattacks.
  - ✓ Only 38% of state and local government employees are trained on general ransomware prevention.
- ✓ Overall, employees largely concur that specialized software and tools, raising awareness of the threats, and specialized training top the list of important prevention measures.
- ✓ On a positive note, two-thirds or more of IT sector employees do report that their organization keeps backups. Most (~two-thirds) also claim that their employer has dedicated security resources.

A majority of employees across sectors recognize their own role in cyberattack prevention, and agree that, as government employees, they have responsibility to help prevent cyberattacks in their communities. That said, many also feel that there is a significant role for the federal government to play.

- ✓ At least 72% of employees across sectors agree that the federal government should provide assistance to communities for damages from cyberattacks.
- ✓ 70% or more also agree that cyberattacks should warrant emergency responses and support similar to those used for natural disasters.

Educators had the lowest amount of cybersecurity training compared to other surveyed state and local professionals. In general, 44% said they hadn't received basic cybersecurity training.

- ✓ 70% said they have not received adequate training on how to respond to a cyberattack.
- ✓ Not surprisingly, their confidence in their own ability to recognize and prevent a ransomware attack is nearly 20% lower than other state and local employees surveyed.

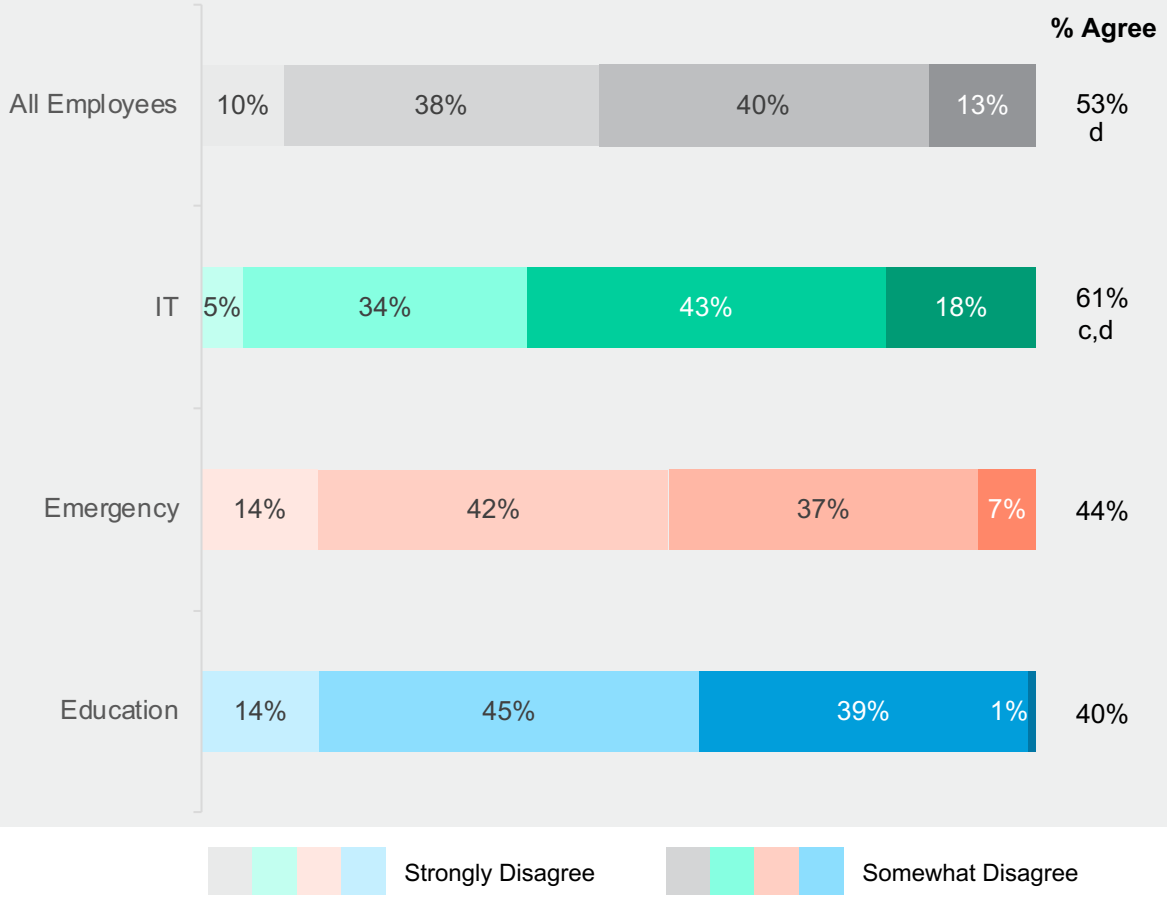
Cybersecurity In The Community

Expectations for community cyberattacks increasing are modest. Concern for the disruption of the election is greater.

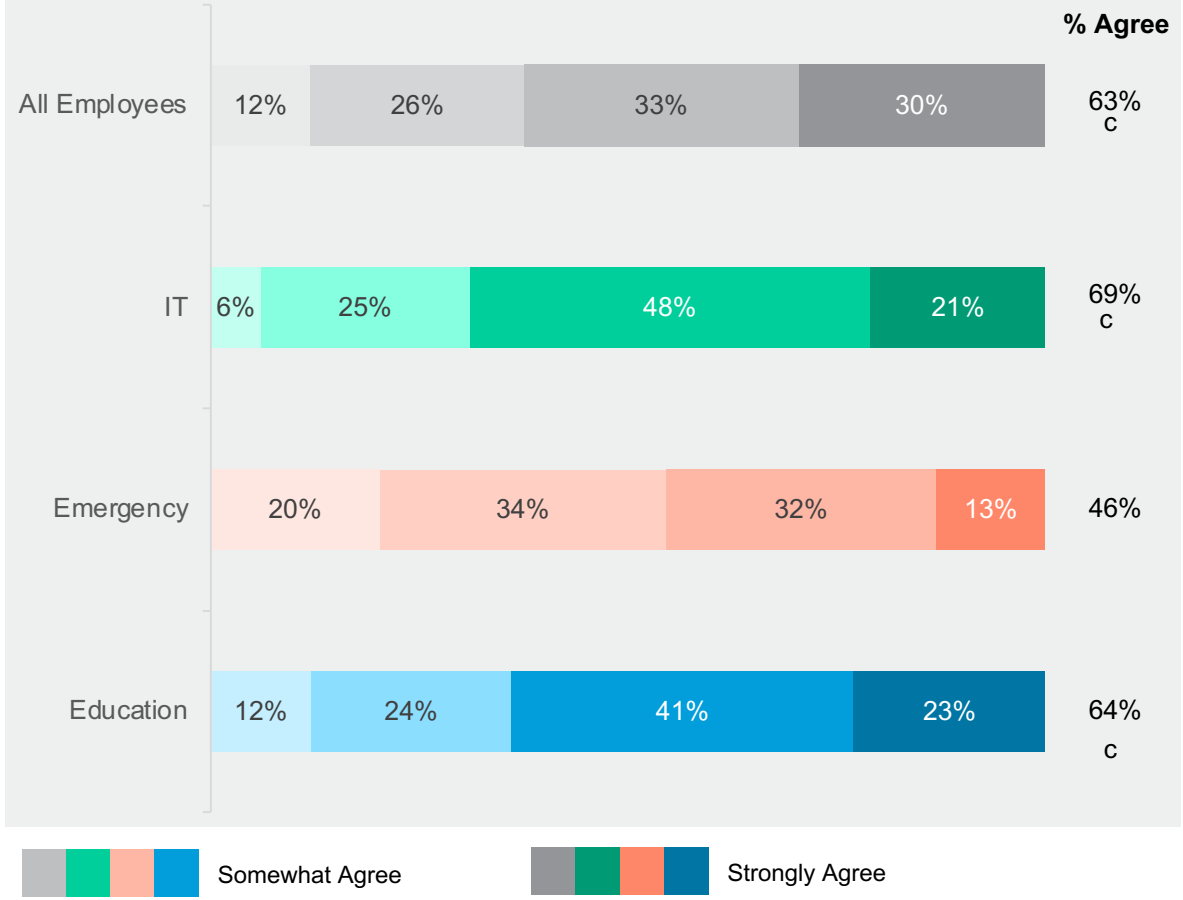
Emergency responders are less likely to expect an increase in attacks and are less concerned than other audiences on election disruption.

All Employees (a) | Emergency (c) | IT (b) | Education (d)

I Expect Cyberattacks Against My Community To Increase Next Year



I Am Concerned Cyberattacks Could Disrupt The 2020 Elections



Letters indicate significance differences between audiences

All Employees (a) | Emergency (c)
IT (b) | Education (d)

Government employees across sectors cite threats against the elections among their top concerns in 2020.

At least 4 in 10 believe systems in their community are vulnerable. Administrative offices fall toward the top of vulnerable systems for most audiences. Meanwhile, those in IT see the greatest vulnerability for utilities.

Vulnerability Of Systems In The Communities Served By Employer




	Vulnerable	Vulnerable	Vulnerable	Vulnerable
Administrative Offices	8% 22% 52% 18% 70%	4% 29% 48% 20% 67%	1% 32% 59% 8% 67%	6% 24% 56% 14% 70%
Local Utility Departments	7% 25% 54% 14% 68%	7% 18% 53% 22% 75%	3% 36% 53% 8% 61%	9% 26% 54% 11% 65%
Board of Elections	10% 25% 39% 26% 65% c	8% 28% 47% 18% 64%	3% 47% 34% 17% 50%	6% 26% 46% 22% 68% c
Public Schools	8% 29% 45% 18% 63%	8% 21% 57% 14% 71%	3% 38% 47% 12% 58%	3% 31% 48% 17% 66%
911 Emergency Services	8% 32% 49% 11% 60%	9% 30% 46% 15% 61%	7% 43% 43% 7% 50%	6% 33% 50% 11% 61%
Transportation	11% 30% 48% 11% 60% c	7% 28% 49% 16% 66% c	7% 47% 40% 6% 46%	10% 28% 50% 12% 62% c
Local Courts	8% 34% 45% 13% 58%	6% 35% 43% 16% 59%	6% 40% 46% 8% 54%	5% 38% 47% 9% 56%
Police Department	10% 36% 45% 10% 54%	9% 36% 41% 15% 56%	4% 44% 44% 8% 52%	7% 28% 50% 15% 65% c
Department of Public Works	10% 39% 40% 11% 51%	9% 37% 39% 16% 55%	12% 41% 34% 13% 47%	15% 36% 43% 6% 48%
Parks and Recreation	13% 42% 35% 10% 45%	15% 41% 34% 10% 44%	15% 45% 33% 8% 41%	17% 38% 35% 9% 45%

Not Vulnerable At All
Not Too Vulnerable
Very Vulnerable
Somewhat Vulnerable

Letters indicate significance differences between audiences

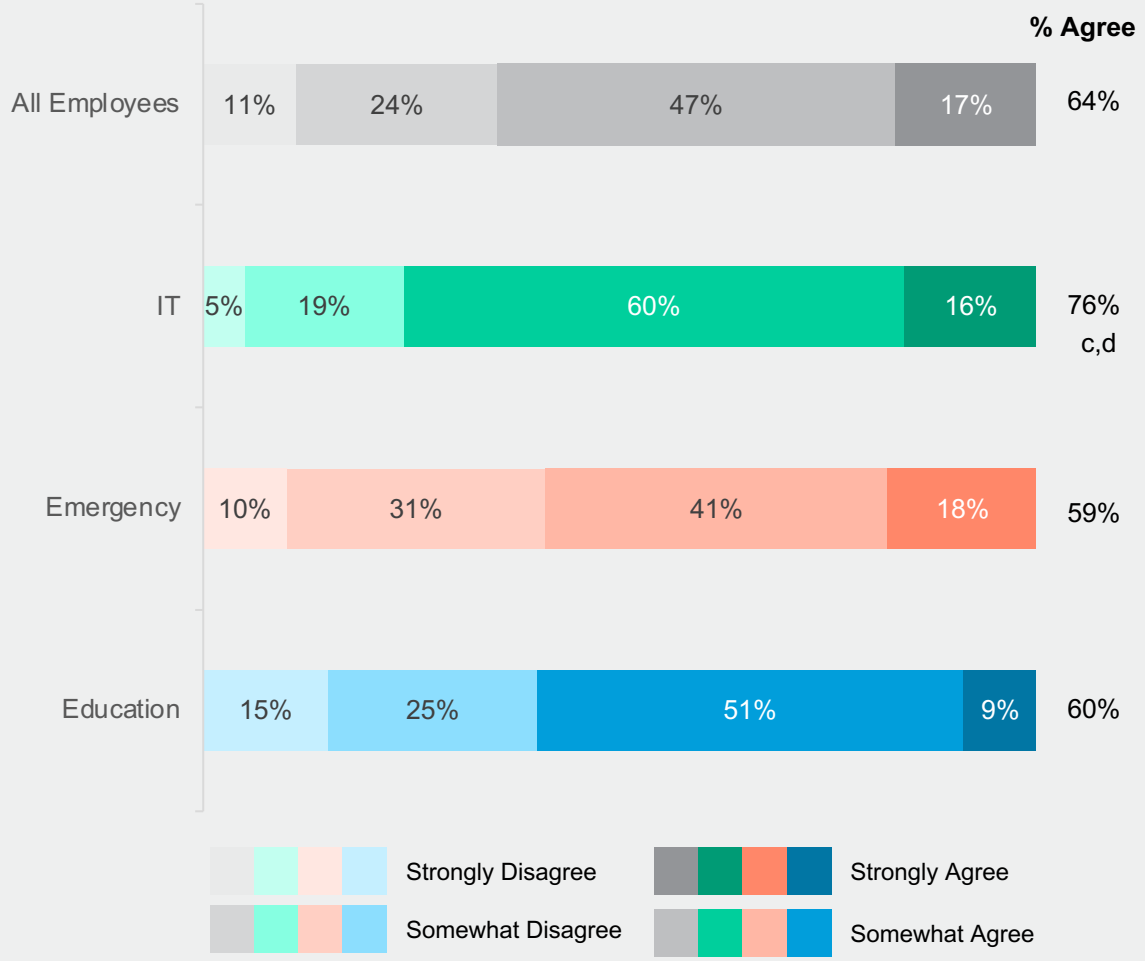
Cybersecurity In The Workplace

At least 6 in 10 can imagine their employer being victim of a cyberattack. However, similar numbers also have confidence in their employer's ability to manage an attack.

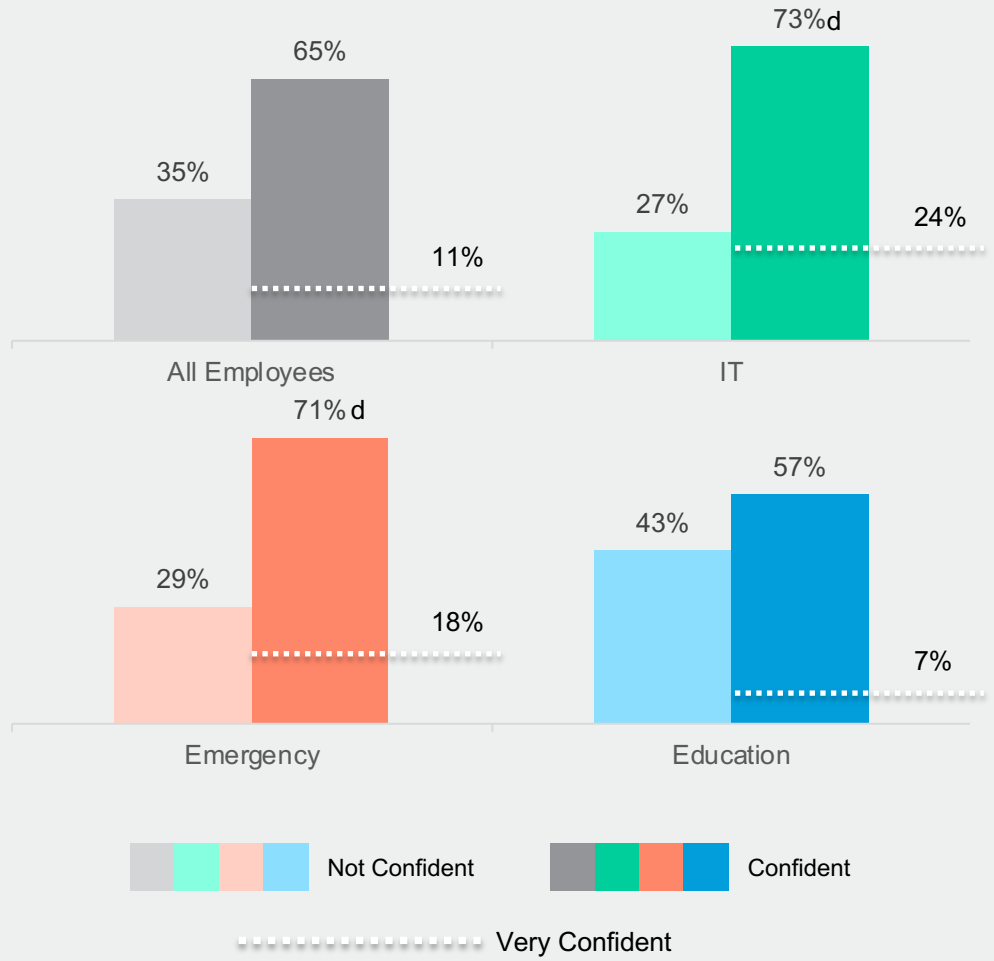
Those in IT are more likely to imagine their employer being a victim. IT and Emergency employees feel most confident in their employer's ability to cope.

All Employees (a) | Emergency (c) | IT (b) | Education (d)

I Can Imagine My Employer Being Victim Of A Cyberattack In The Future



Confidence In Employer's Ability To Manage The Consequences From A Cyberattack



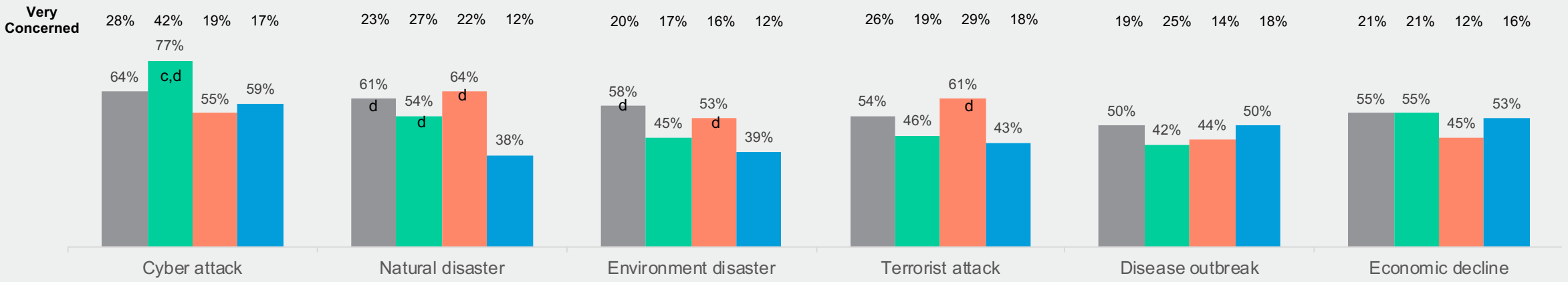
Letters indicate significance differences between audiences

Three out of four audiences express more concern for cyberattacks than any other threat.

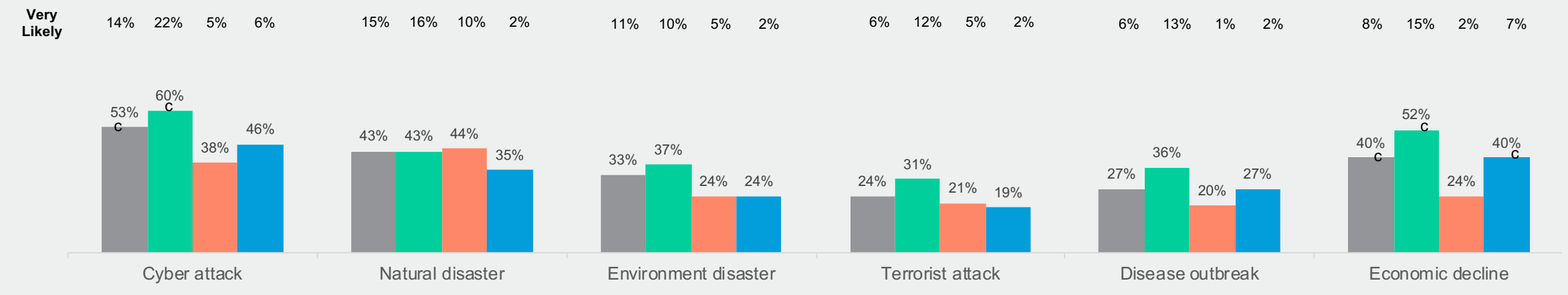
All Employees (a) | Emergency (c) | IT (b) | Education (d)

However, although concern about cyberattacks is high, employees across sectors are somewhat less likely to believe an attack will happen within the next year.

Somewhat/Very Concerned About Threats Affecting Employer



Believe Employer Is Somewhat/Very Likely To Deal With Threats In The Next Year



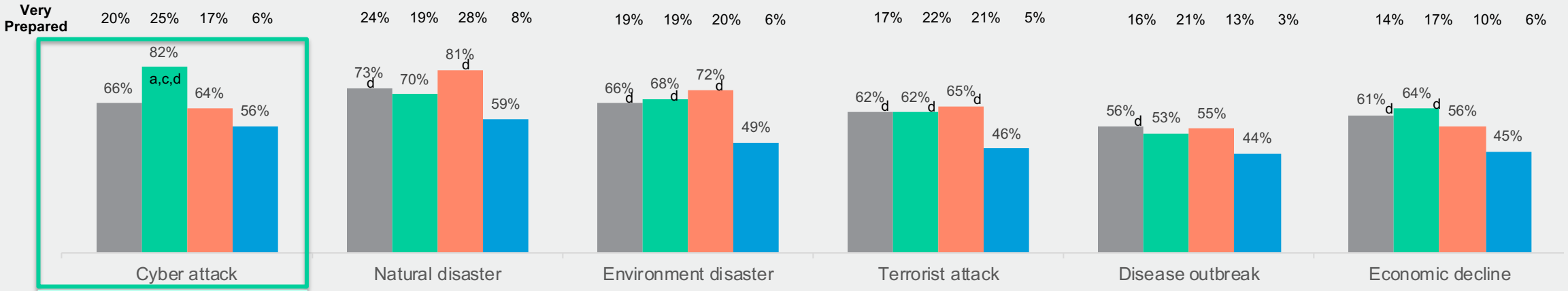
Letters indicate significance differences between audiences

For all possible threats to a community, government employees feel at least somewhat prepared.

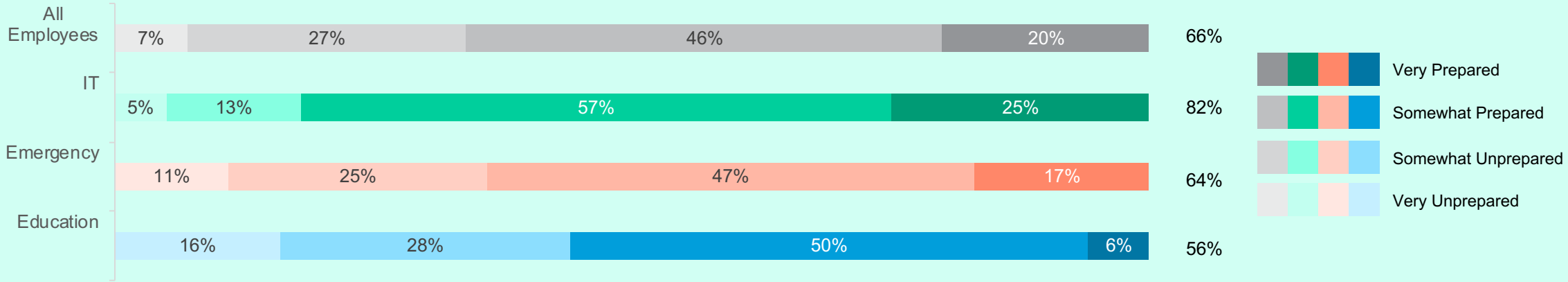
Those in IT feel particularly prepared to handle cyberattacks. Meanwhile, Education employees are noticeably less confident across the board.

All Employees (a) | Emergency (c) | IT (b) | Education (d)

Employer Is Somewhat/Very Prepared To Deal With Threats Affecting The Services It Provides To Communities



Employer Preparedness To Deal With A Cyberattack



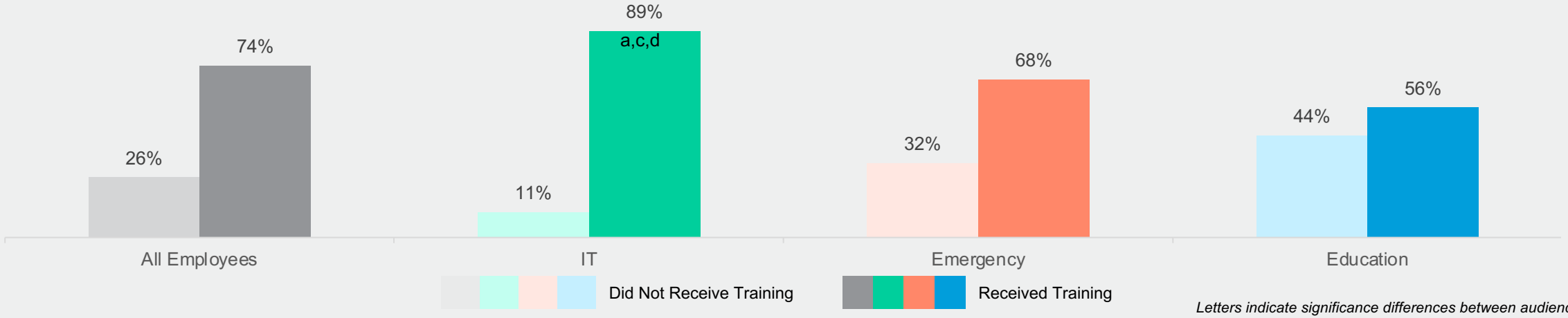
Letters indicate significance differences between audiences

One in four from the "All Employees" audience have not received any kind of basic cybersecurity training. Education sector employees lag considerably with respect to training.

Government employees who did receive training often feel that their employer is more prepared to deal with a cyberattack.

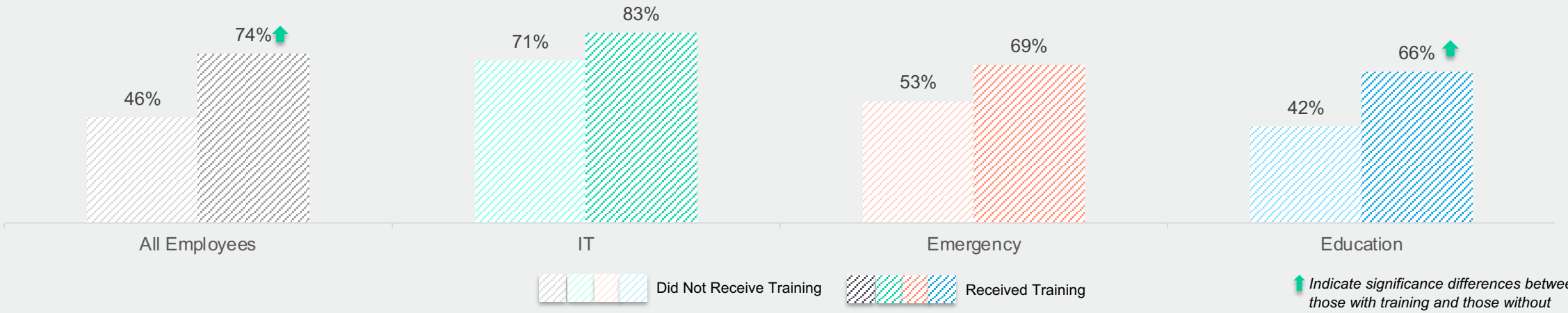
All Employees (a) | Emergency (c) | IT (b) | Education (d)

Received Some Type Of Cybersecurity Training Versus Received No Training



Letters indicate significance differences between audiences

Employer Is Somewhat/Very Prepared To Deal With A Cyberattack – Trained vs Not Trained



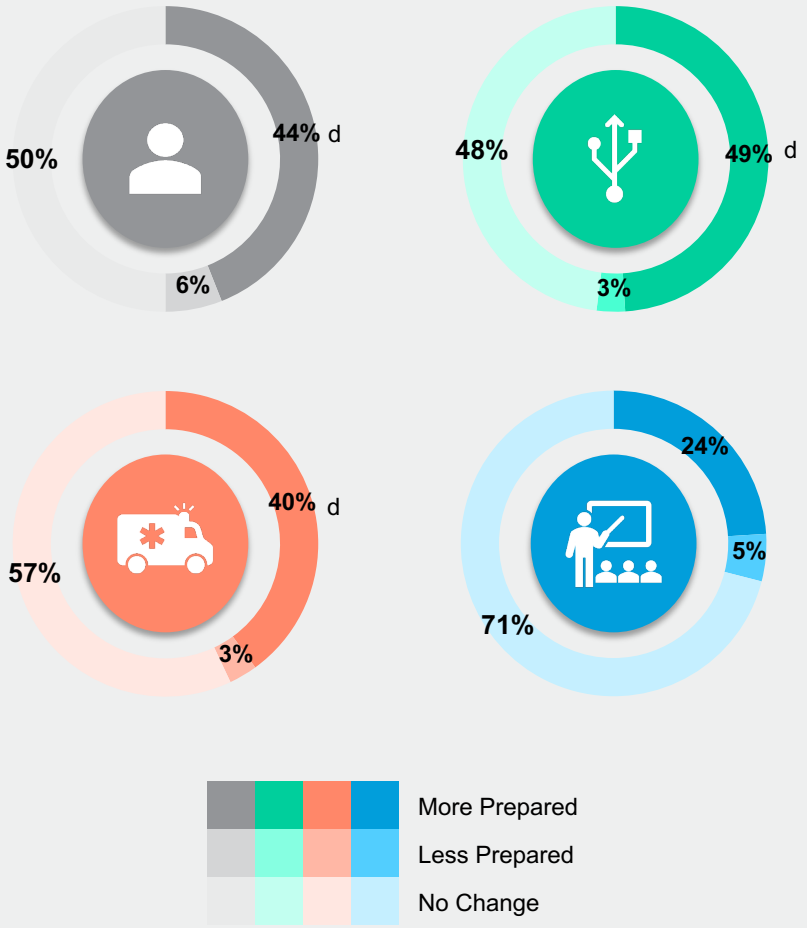
Indicate significance differences between those with training and those without

39% or more government employees say they do not expect any change in budget and resources dedicated to managing the threat of cyberattacks.

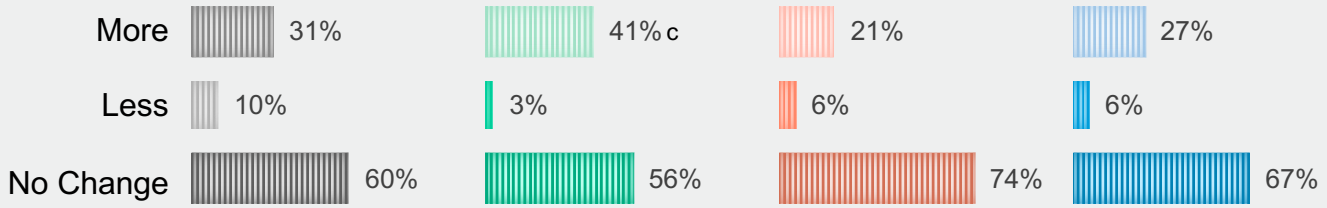
That said, at least 25% of government employees do feel that their employer is more prepared compared to last year.

All Employees (a) | Emergency (c) | IT (b) | Education (d)

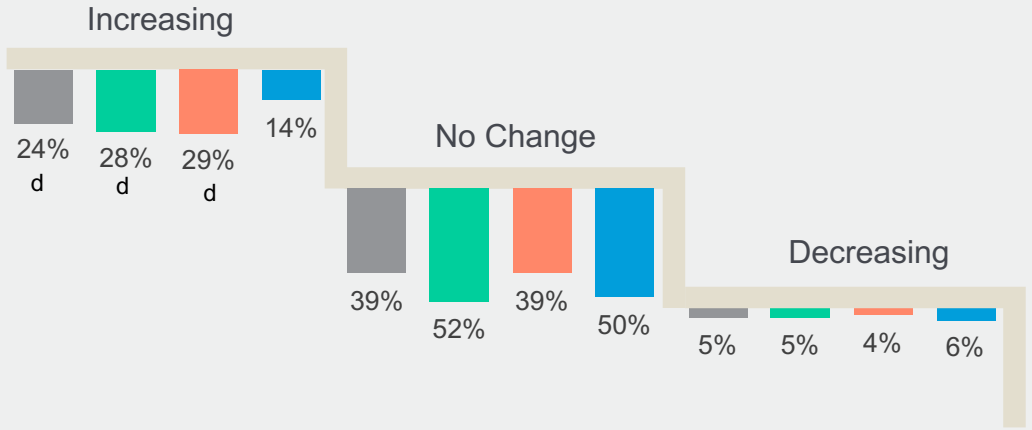
Employer Preparedness To Deal With The Threat Of Cyberattacks Compared To Last Year



Concern About Cybersecurity And Cyberattacks On Employer Compared To Last Year



Employer Action On Budget And Resources Dedicated To Managing The Threat Of Cyberattacks



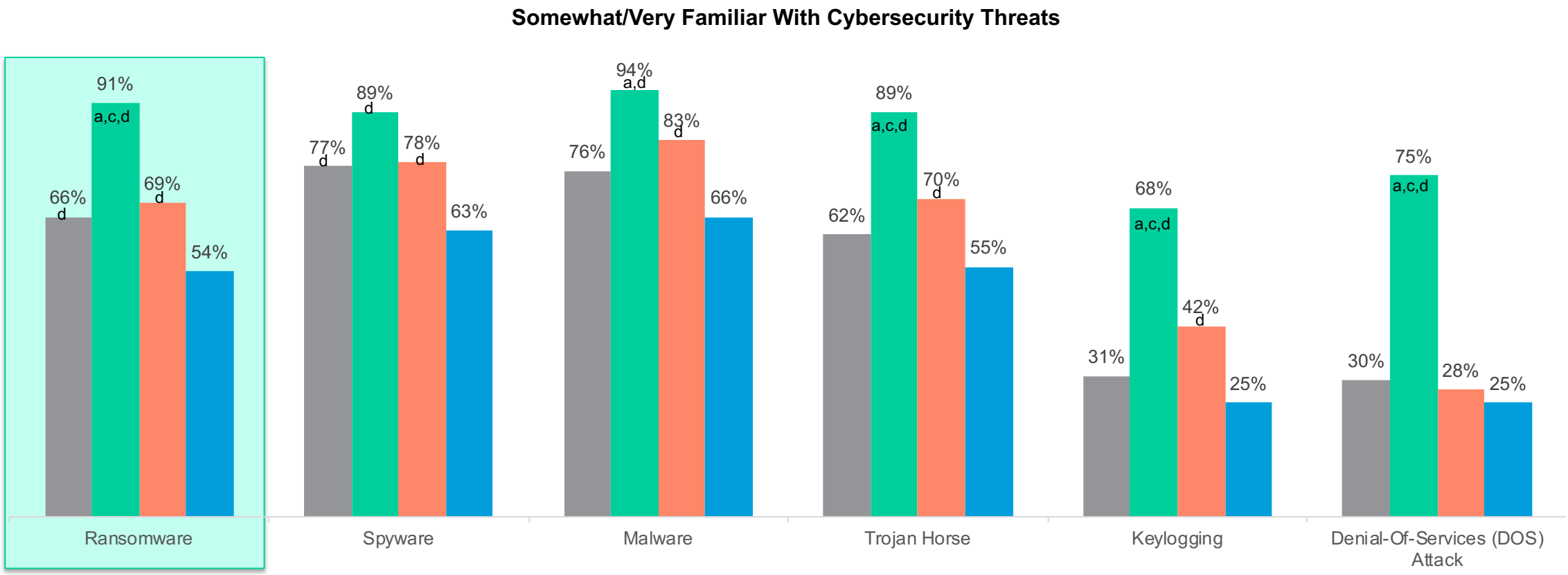
Letters indicate significance differences between audiences

Ransomware

All Employees (a) | Emergency (c) | IT (b) | Education (d)

Ransomware familiarity is high, often only behind Spyware and Malware.

66% of ‘All Employees’ are aware of Ransomware, by far outpacing familiarity with Keylogging and Denial-Of-Services (DOS) attack. Familiarity consistently lags among the Education sector.



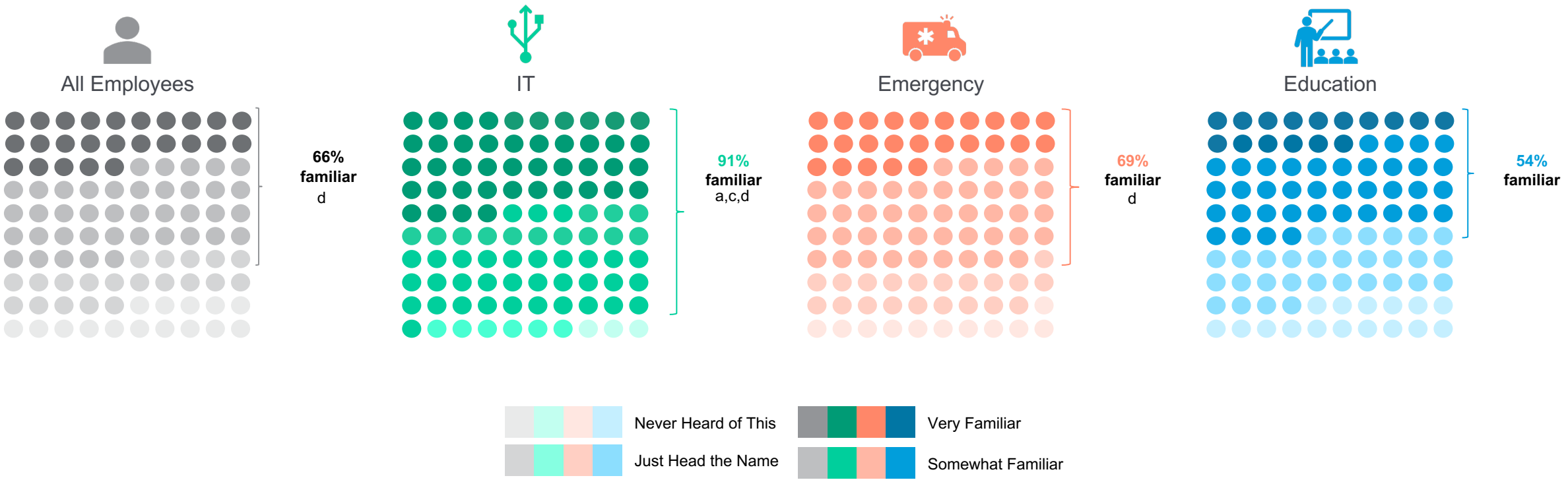
Letters indicate significance differences between audiences

All Employees (a) | Emergency (c) | IT (b) | Education (d)

A more granular deep dive exposes a high level of ransomware unawareness for Education sector employees.

Three in ten Education employees have just heard the name ‘Ransomware’ compared to 2 in 10 of Emergency and “All Employees.” IT employees, expectedly, show near universal awareness.

Familiarity With Ransomware



Letters indicate significance differences between audiences

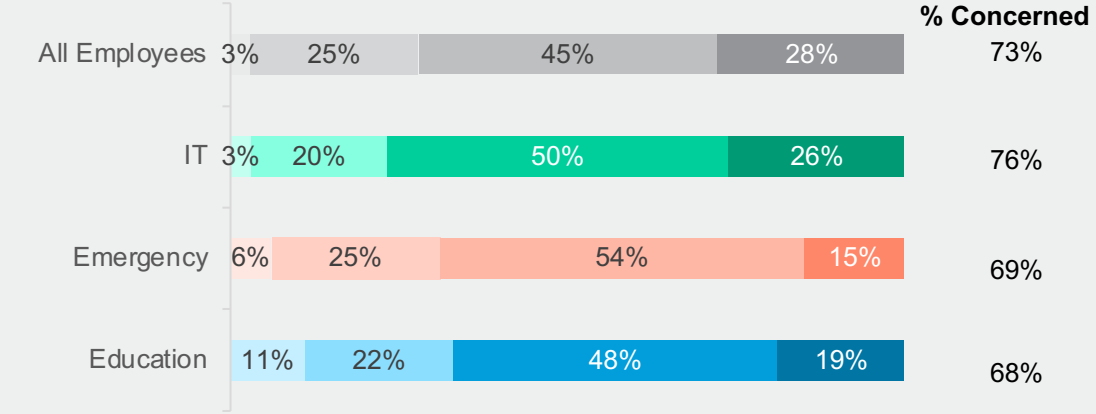
RANSOMWARE

The threat of ransomware attacks feels real to government employees across sectors.

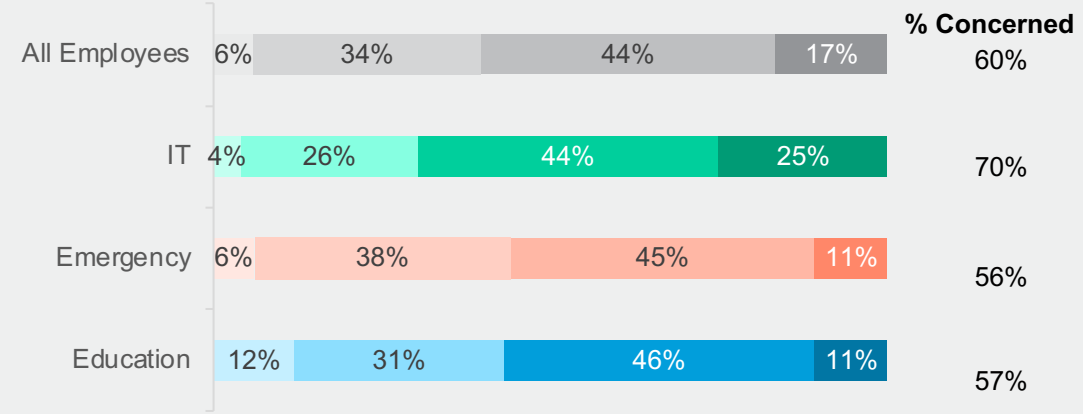
That said, their concern is greatest for attacks against the U.S., their cities and personal data; less for their own department at work.

All Employees (a) | Emergency (c) | IT (b) | Education (d)

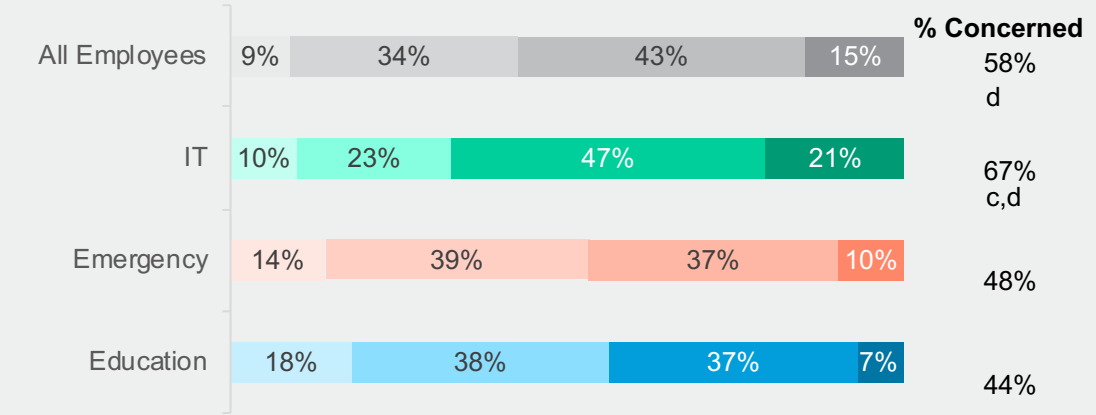
Concern About The Threat Of Ransomware To Cities Across The US



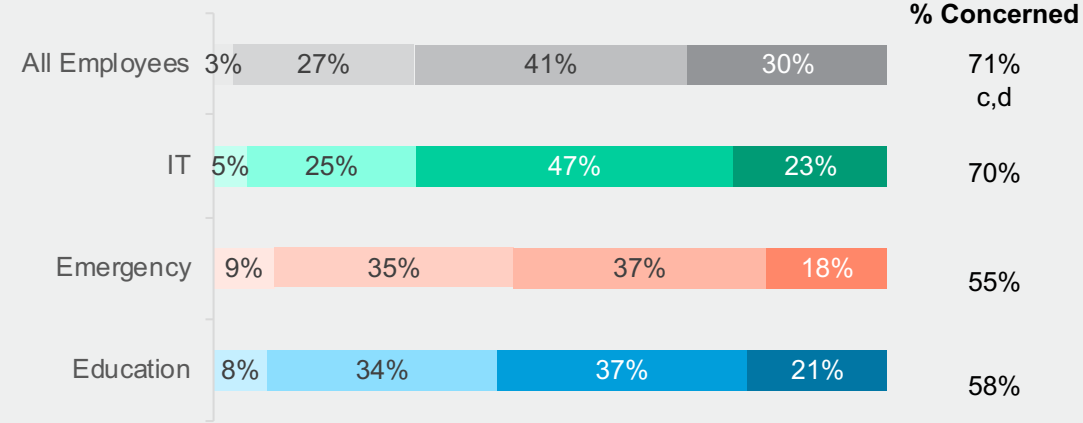
Concern About The Threat Of Ransomware To Their City/County/Town



Concern About The Threat Of Ransomware To Their Department At Work



Concern About The Threat Of Ransomware To Their Personal Data



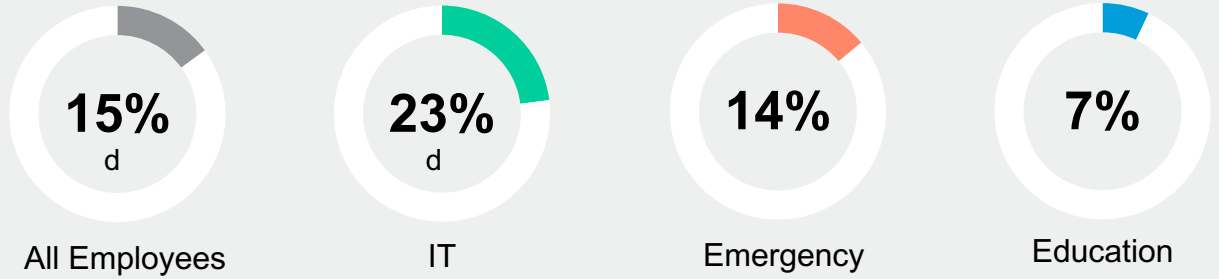
Not Concerned At All | Not Too Concerned | Somewhat Concerned | Very Concerned

One in six of “All Employees” say their department has been hit with a ransomware attack.

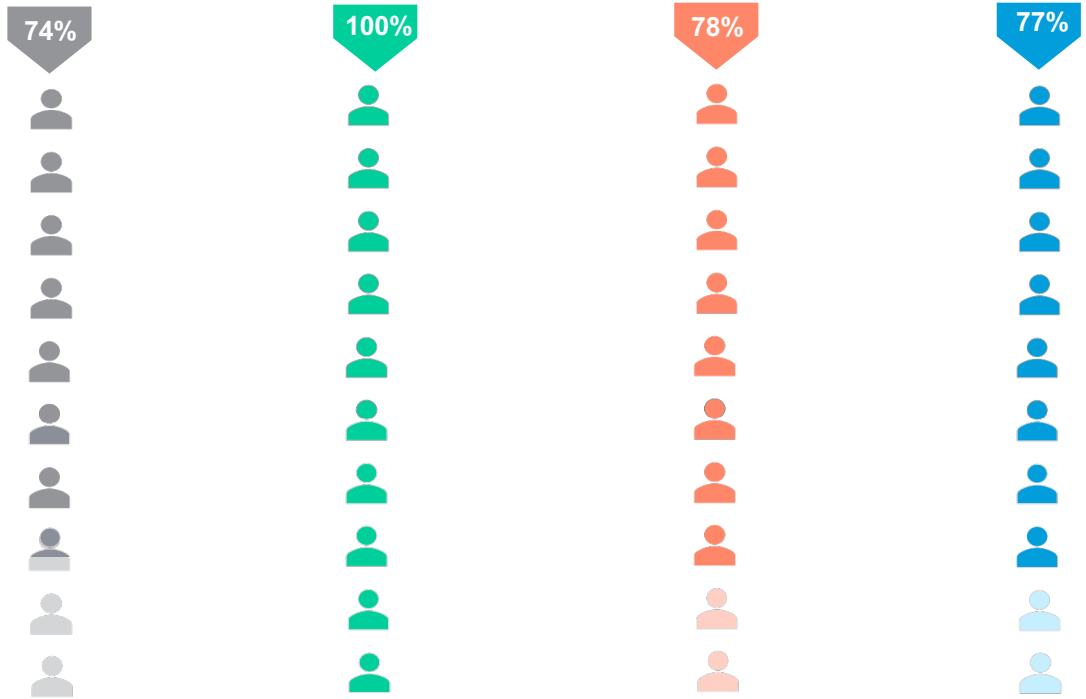
A strong majority of these employees believe their employer was successful at handling the attack.

All Employees (a) | Emergency (c) | IT (b) | Education (d)

Employer Has Been The Target Of A Ransomware Attack



Employer Was Successful At Handling The Ransomware Attack*



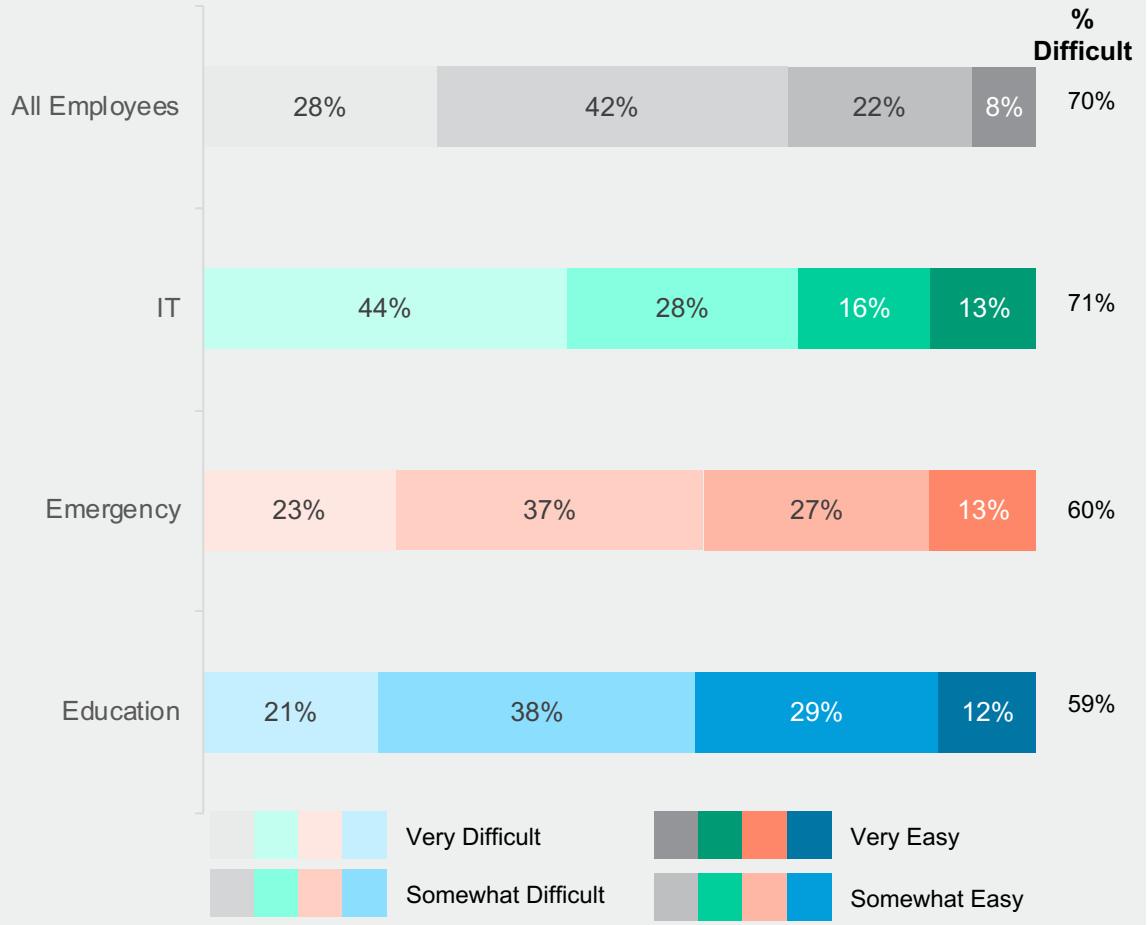
Letters indicate significance differences between audiences
**Small bases.*

At least six in ten government employees across departments claim a ransomware attack would make doing their jobs difficult.

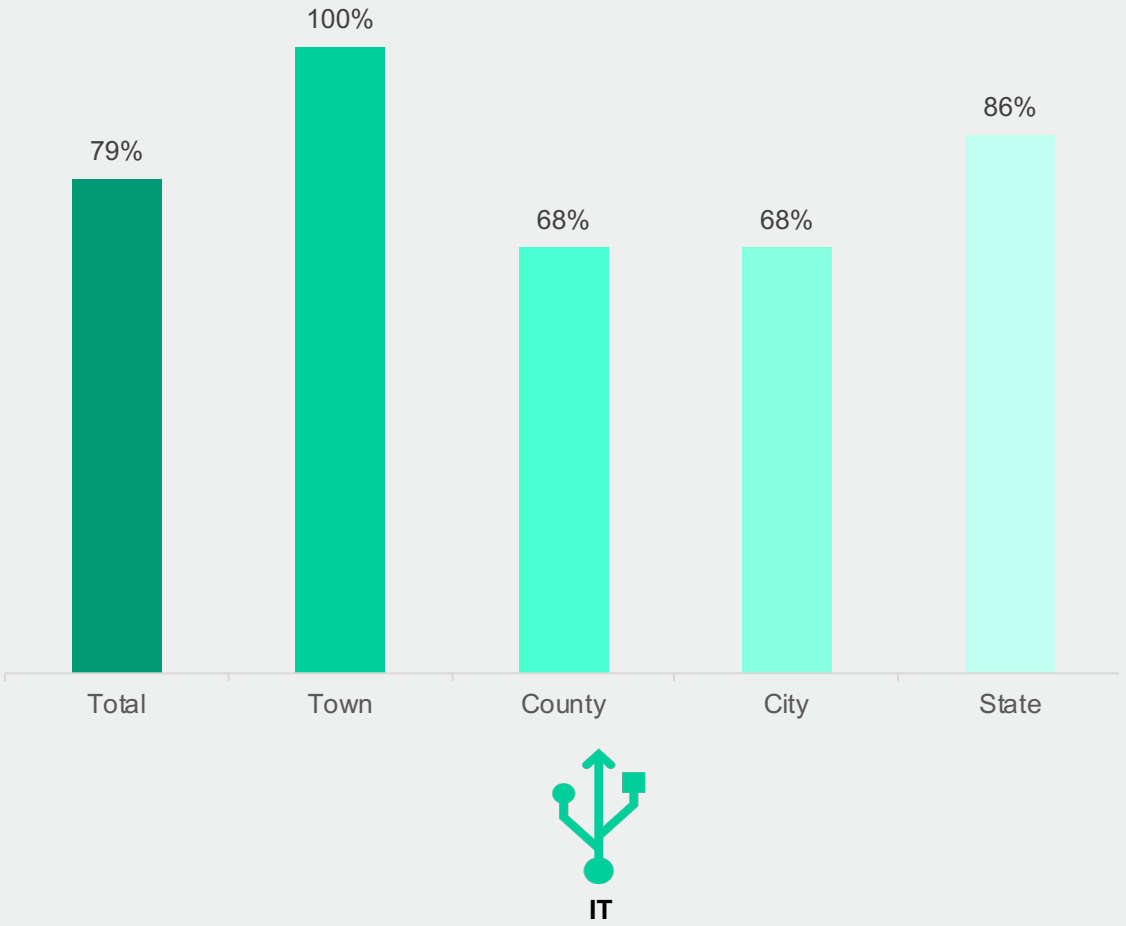
A large majority of IT employees state their organization maintains paper or digital backups, but in the event of a Ransomware attack, 44% say their job would still be very difficult even using these backups.

All Employees (a) | Emergency (c) | IT (b) | Education (d)

Ease Of Doing Job If Department Was Hit With A Ransomware Attack



Somewhat / Strongly Agree: My Organization Maintains Paper Or Digital Backups



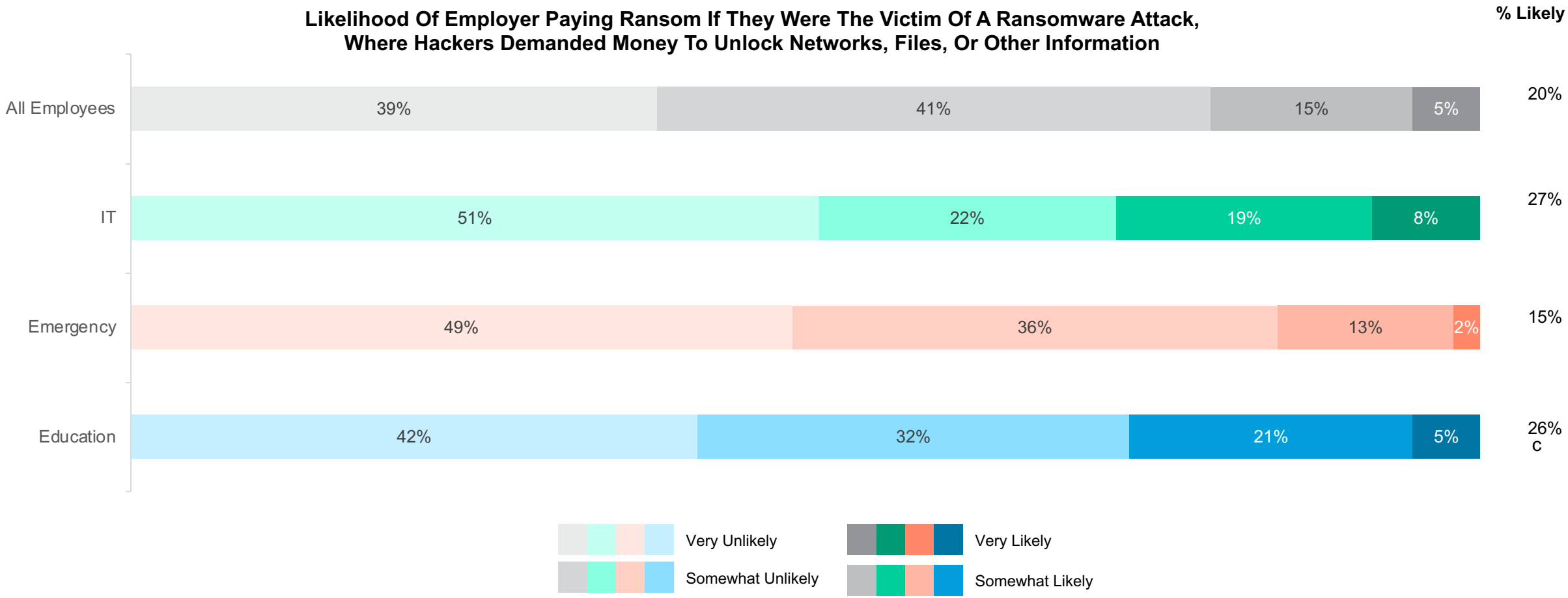
Letters indicate significance differences between audiences

All Employees (a) | Emergency (c) | IT (b) | Education (d)

Government employees across departments are not likely to think their employer would pay a ransom in the event of an attack.

A strong majority of government employees believe it is somewhat or very unlikely that their employer would pay a ransom.

Likelihood Of Employer Paying Ransom If They Were The Victim Of A Ransomware Attack, Where Hackers Demanded Money To Unlock Networks, Files, Or Other Information



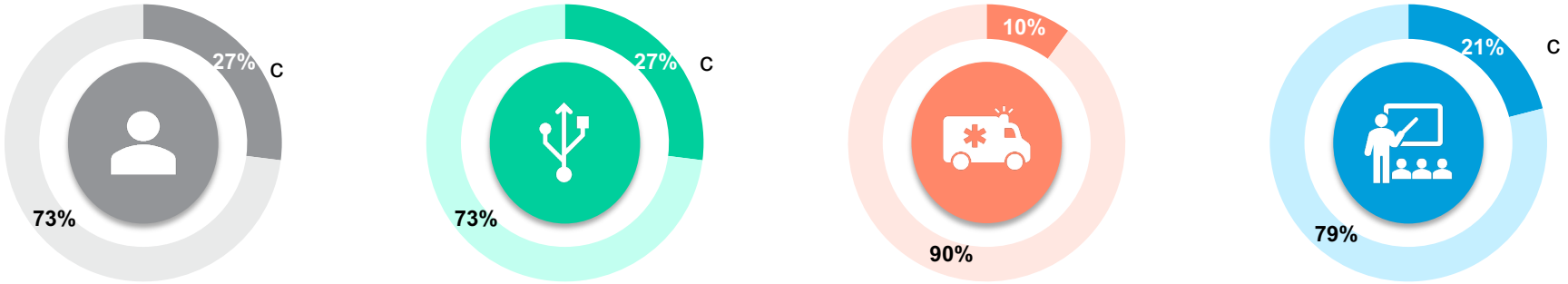
Letters indicate significance differences between audiences

All Employees (a) | Emergency (c)
IT (b) | Education (d)

Government employees across departments would rather incur higher recovery costs than pay a ransom.

Emergency sector employees are significantly more likely to be against paying a ransom than other government employees.

Given An Option, Preference Between Not Paying A Ransom, But Paying Higher Repair Costs To Get Systems Up And Running, Or Paying A Ransom And Saving Taxpayer Dollars



Paying A Ransom, But Saving Taxpayer Dollars

Not Paying A Ransom, But Paying Higher Repair Costs

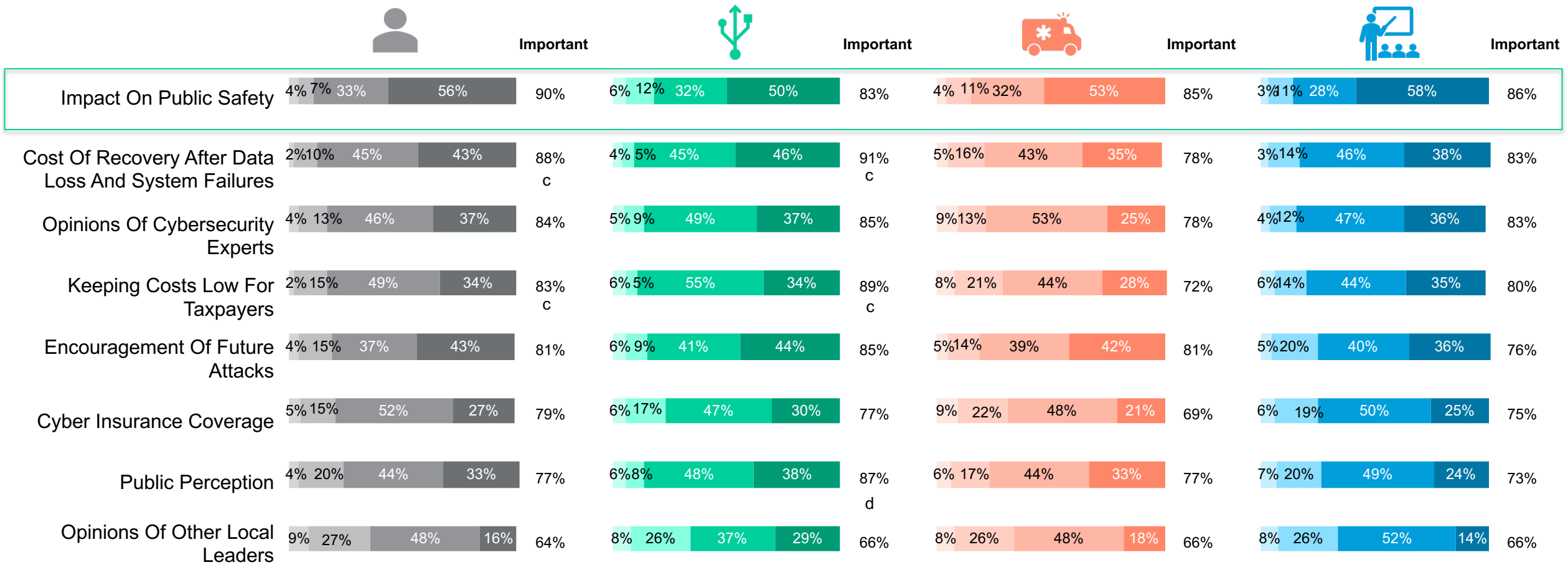
Letters indicate significance differences between audiences

All Employees (a) | Emergency (c)
IT (b) | Education (d)

Not surprisingly, 50% or more employees across departments believe impact on public safety should be a very important consideration in deciding whether to pay ransom.

Cost of recovery after data loss and system failures and encouragement of future attacks are also considered very important factors for all. Opinion of local leaders and public perception (though still important, especially among IT sector employees) are of relatively lesser importance.

Importance Of Factors For Employer To Consider When Deciding Whether Or Not To Pay Ransom For An Attack Impacting The Community



Letters indicate significance differences between audiences

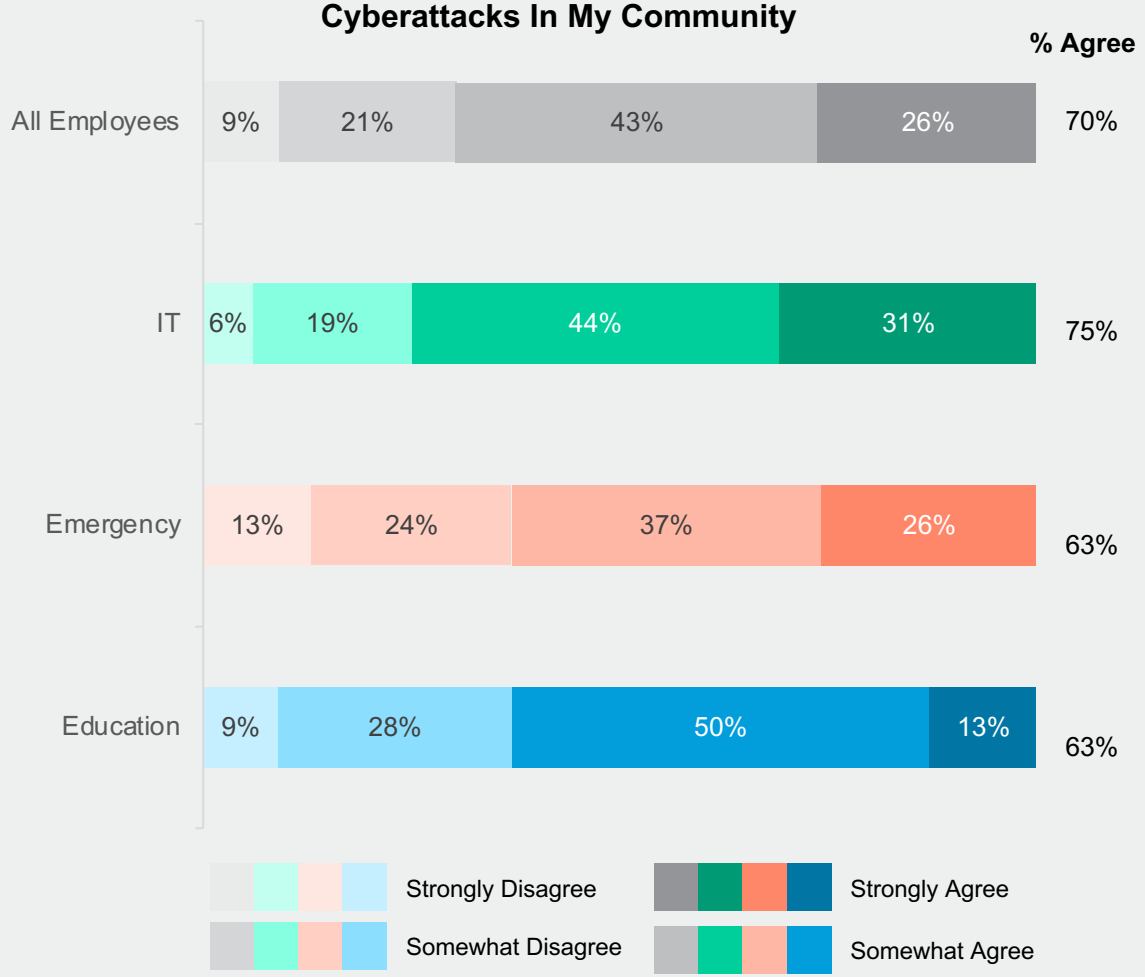
Responsibility And Prevention

All Employees (a) | Emergency (c) | IT (b) | Education (d)

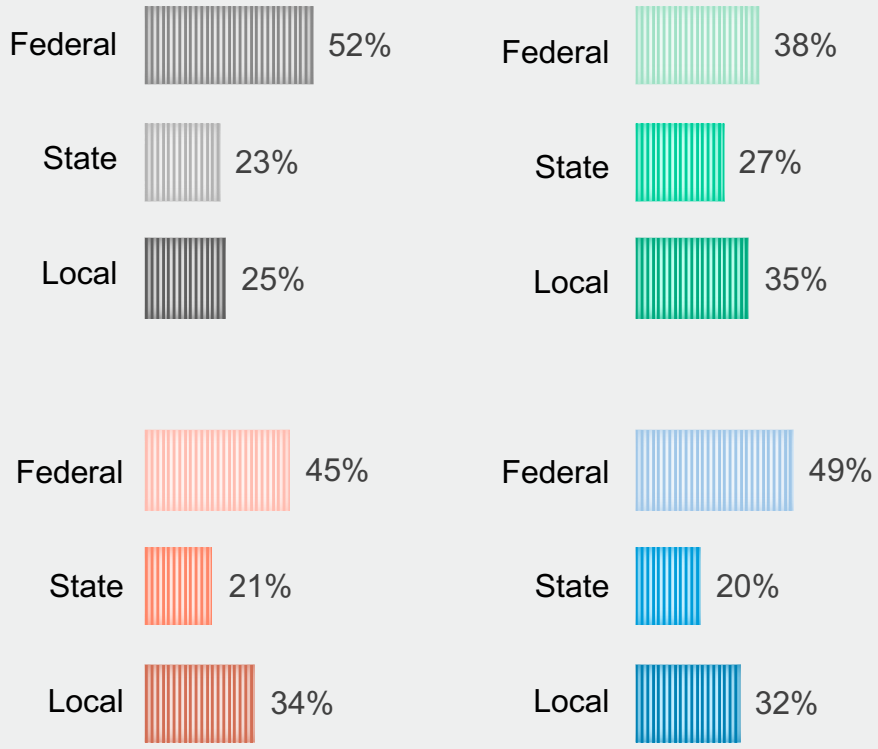
Over 6 in 10 local and state government employees feel they have a personal responsibility to prevent cyberattacks. Many, however, count heavily on the federal government.

Those in IT see this responsibility as shared almost equally across all government bodies.

As A Public Sector Employee, I Have A Responsibility To Help Prevent Cyberattacks In My Community



Government Thought To Have The Greatest Responsibility To Protect Communities From Cyber Attacks



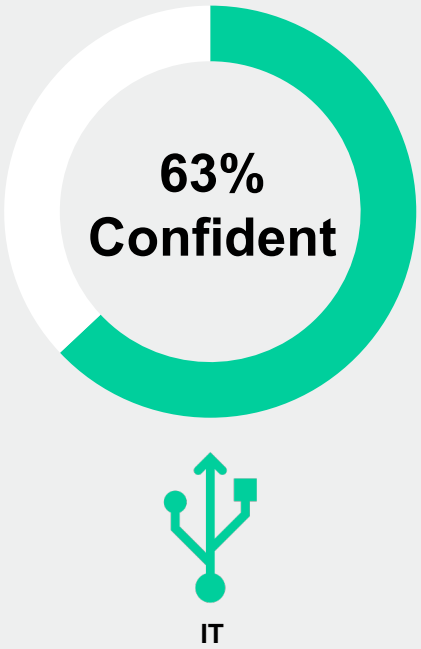
Letters indicate significance differences between audiences

Government employees are largely confident in their ability to recognize and prevent attacks. IT employees mostly agree – though their confidence in their peers is more tempered.

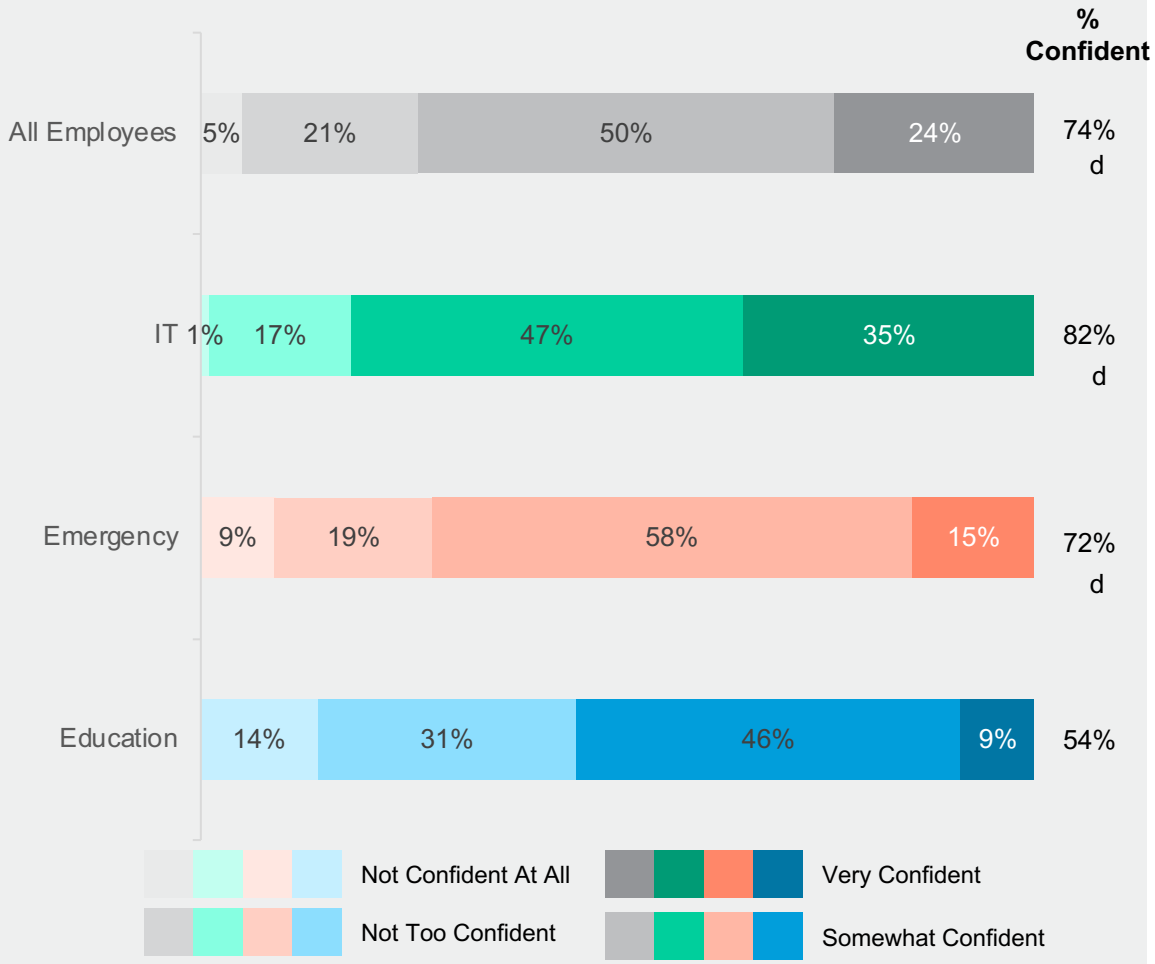
Perhaps evidence of a need for more training, Education sector employees are less confident than others in their own abilities.

All Employees (a) | Emergency (c) | IT (b) | Education (d)

IT Professionals Somewhat/Very Confident That Others In Their Organization Would Be Able To Recognize/Prevent A Ransomware Attack



Confidence In Ability To Recognize And Prevent A Ransomware Attack

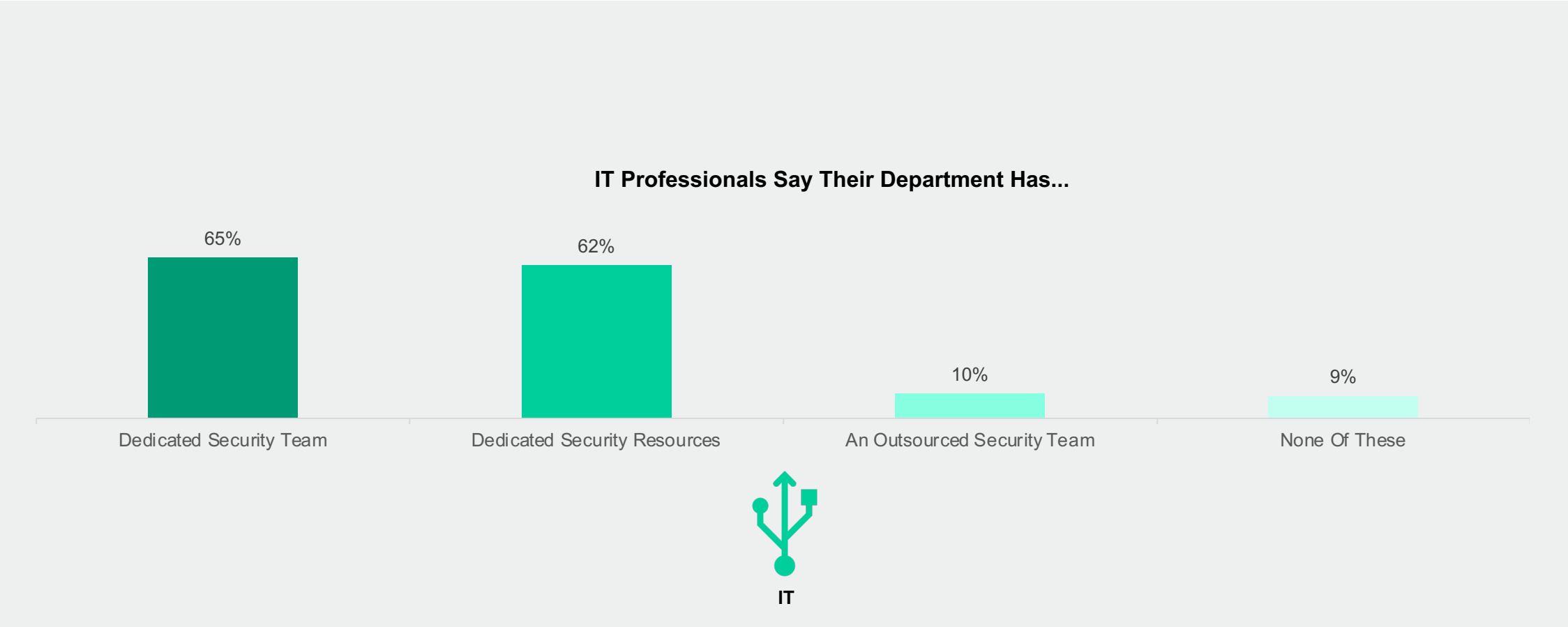


Letters indicate significance differences between audiences

IT (b)

Dedicated resources are reported by 6 in 10 IT employees.

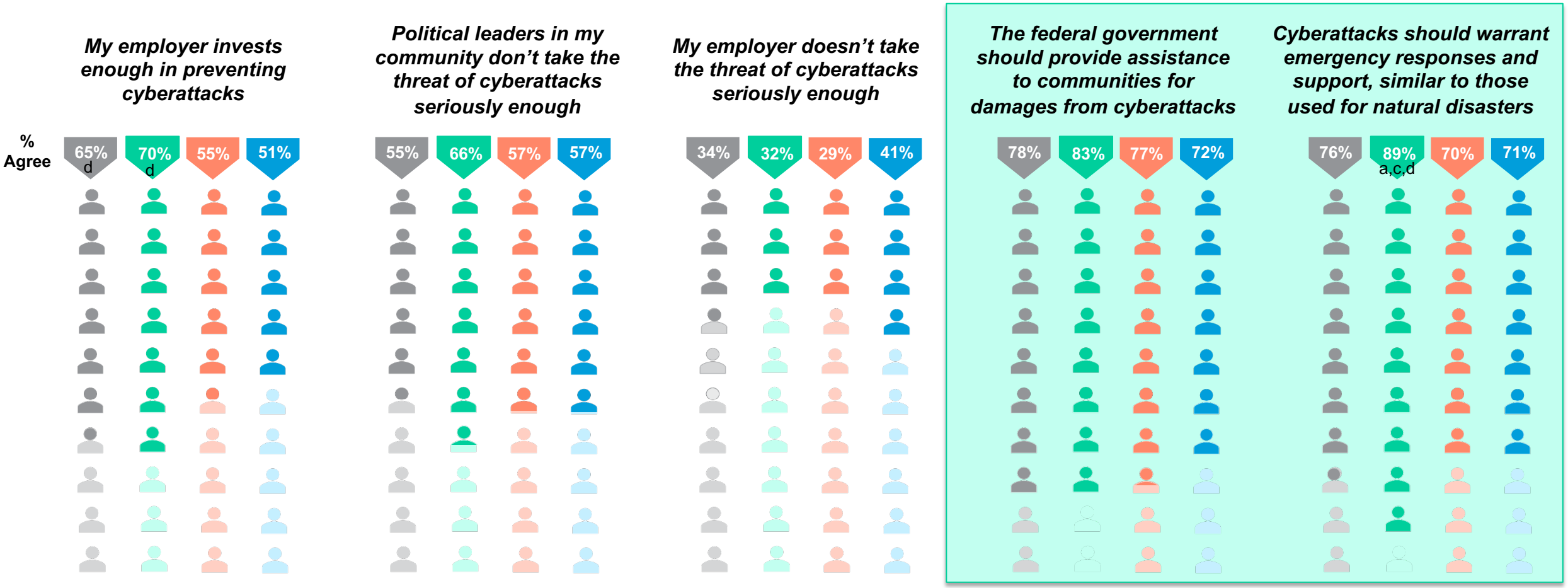
Somewhat concerning, is that one in ten IT professionals say their departments do not have any sort of dedicated or outsourced security team.



All Employees (a) | Emergency (c) | IT (b) | Education (d)

A strong majority of government employees agree cyberattacks warrant emergency response/support similar to natural disasters along with federal assistance handling damages.

However, over 3 in 10 don't feel their employer takes the threat of cyberattacks seriously enough.



Letters indicate significance differences between audiences

All Employees (a) | Emergency (c) | IT (b) | Education (d)

Government employees believe that specialized software/tools, training, and raising overall awareness of ransomware are most important to battle cybercrime in 2020.

Those in IT feel more budget and funding is also very important.

Importance To Employer In Helping To Prevent Ransomware And Manage The Threat Of Cyberattacks




	Important	Important	Important	Important
Specialized Software And Tools To Help Prevent Cyberattacks	2% 5% 38% 55% — 92%	4% 6% 38% 53% — 90%	3% 13% 35% 49% — 84%	11% 34% 55% — 89%
Raising Awareness About The Threat Of Cyberattacks	3% 7% 40% 50% — 90% c	3% 8% 32% 56% — 89%	3% 16% 33% 47% — 80%	1% 11% 51% 38% — 88%
Specialized Training For Public Employees	5% 9% 40% 47% — 87%	3% 7% 40% 50% — 90%	6% 9% 36% 49% — 85%	17% 42% 41% — 83%
Hiring Specialized Employees To Manage The Threat	5% 10% 45% 40% — 85%	4% 13% 50% 33% — 83%	5% 20% 44% 31% — 75%	2% 14% 49% 34% — 83%
More Support From The Federal Government	3% 12% 42% 42% — 84% c	4% 17% 41% 38% — 80%	6% 22% 50% 22% — 72%	5% 20% 43% 33% — 75%
More Funding And Budget	5% 11% 48% 35% — 83%	4% 9% 37% 50% — 87%	4% 17% 48% 31% — 78%	3% 12% 58% 27% — 85%
More Support From Elected Officials	6% 15% 48% 31% — 79% c	5% 18% 38% 38% — 77%	8% 28% 38% 25% — 64%	5% 23% 54% 18% — 72%

Not Important At All | Not Too Important | Somewhat Important | Very Important

Letters indicate significance differences between audiences

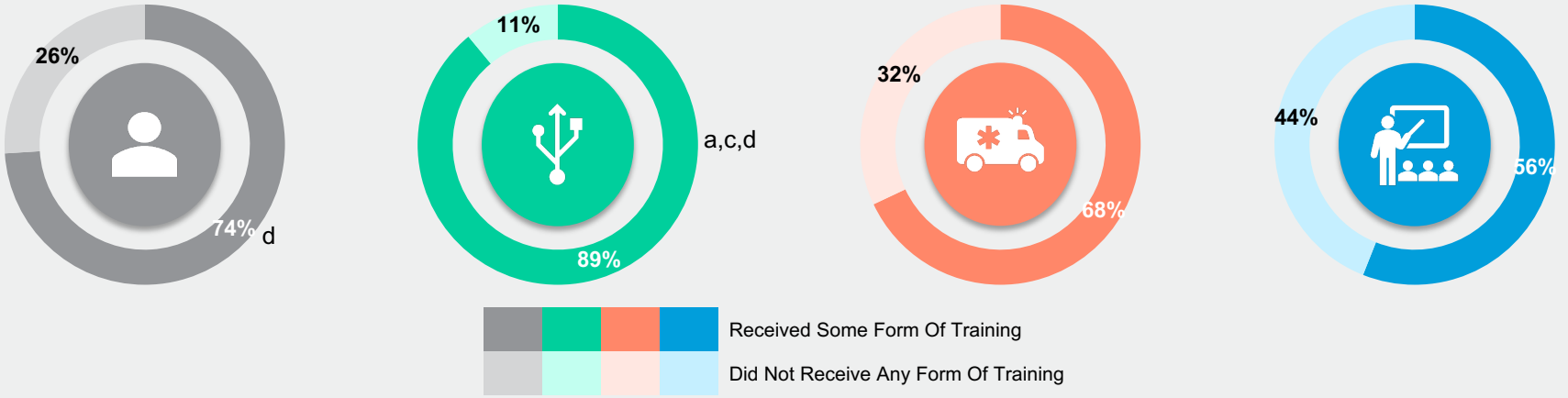
Cybersecurity Training

A majority of government employees have received at least some form of basic cybersecurity training.

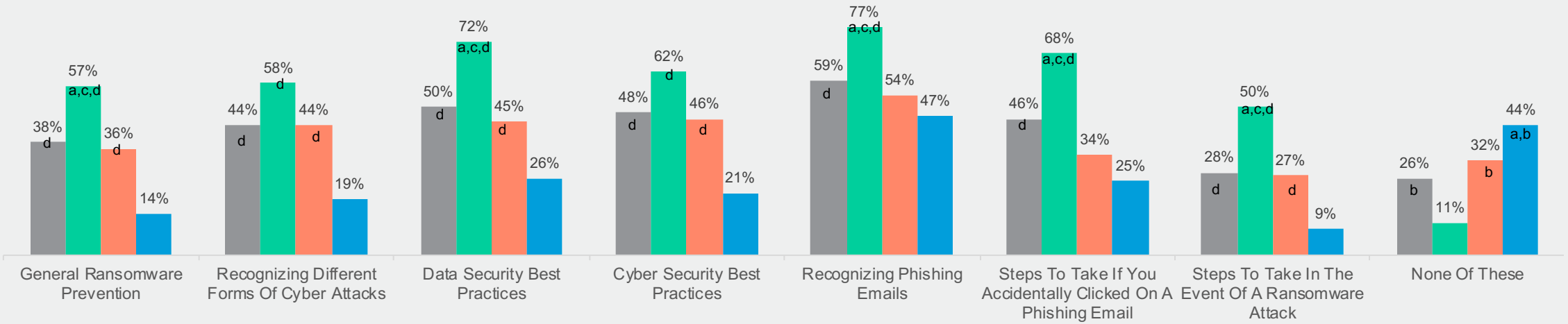
As expected, training is highest among IT employees. Meanwhile, Education sector employees lag other departments consistently.

All Employees (a) | Emergency (c) | IT (b) | Education (d)

Received Some Form Of Training Versus None



Has Received Training

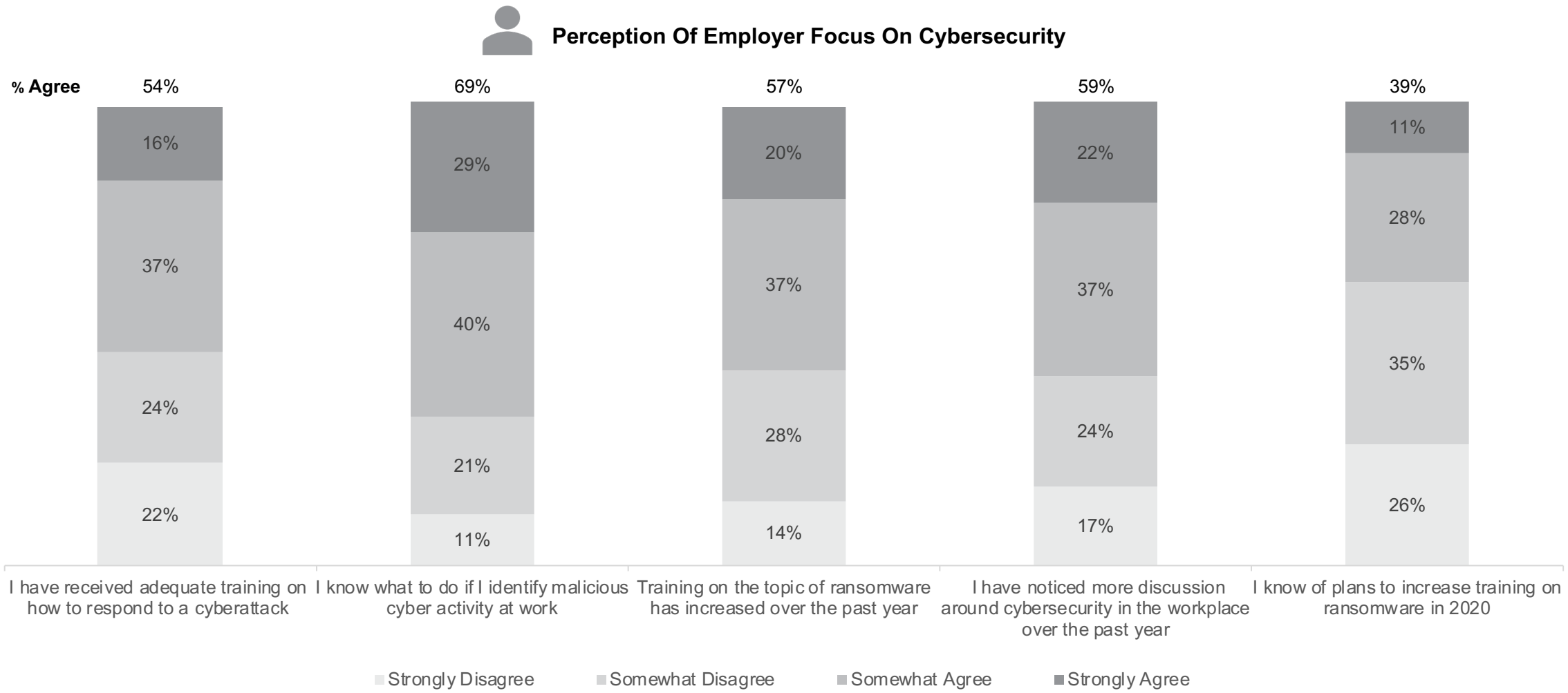


Letters indicate significance differences between audiences

All Employees (a)

Only about half of “All Employees” agree they have received adequate training on how to respond to a cyberattack.

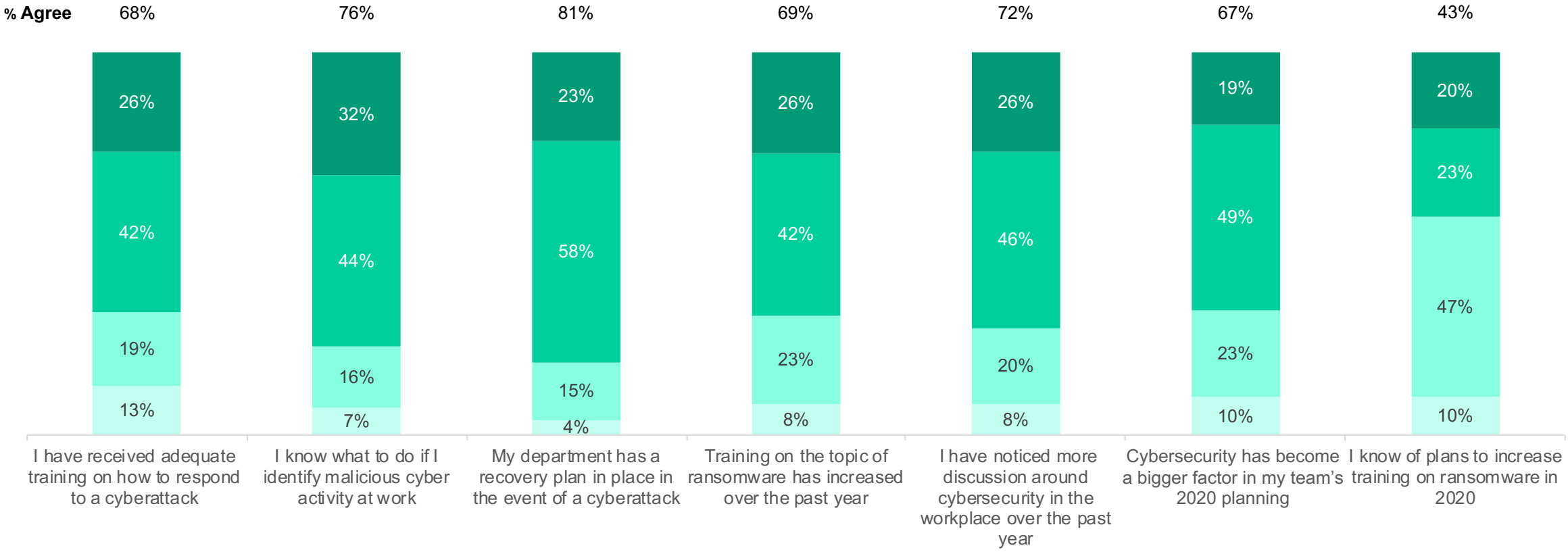
Though there is agreement that training and discussion of ransomware increased in the past year; a majority aren’t aware of plans to increase training in 2020.



Government employees in IT notice more discussion and training around cybersecurity but are not as aware of plans to increase training on ransomware in 2020.

There is high agreement that IT professionals know how to identify a ransomware attack and that their department has recovery plans in place in the event of a cyber attack.

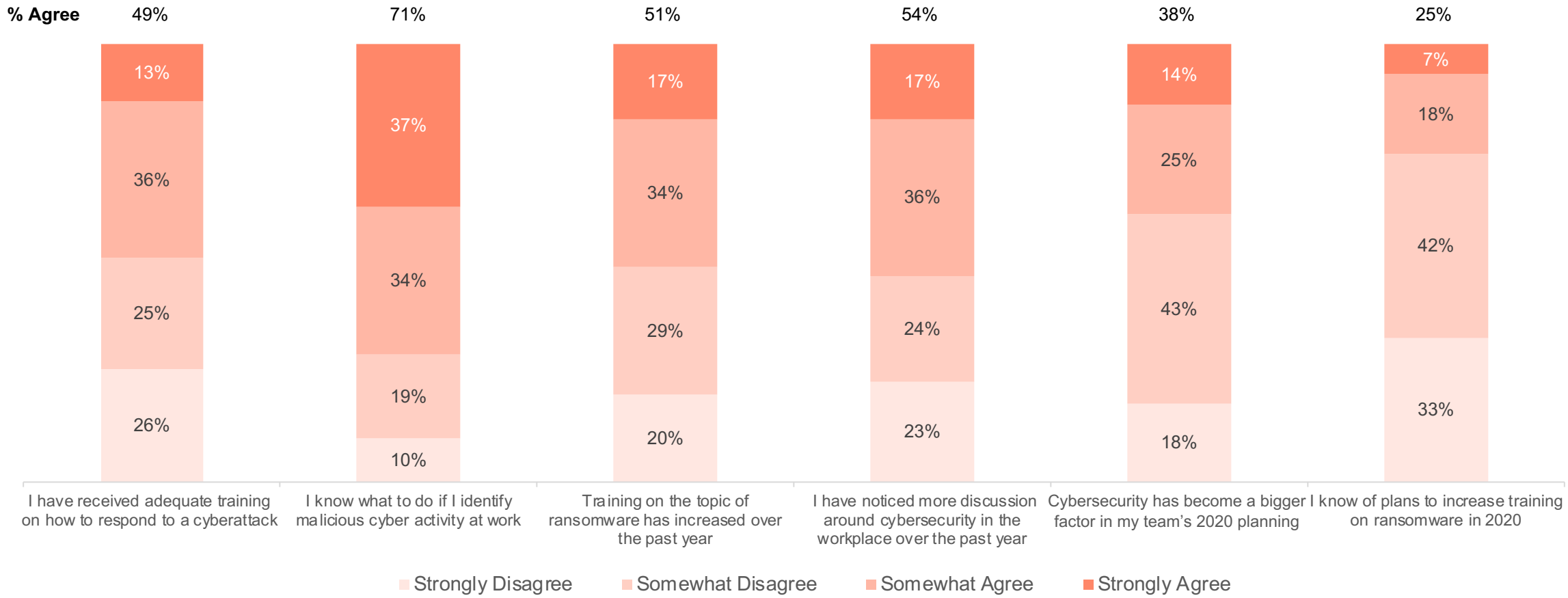
Perception Of Employer Focus On Cybersecurity



Emergency responders' agreement that their employer is focused on cybersecurity issues is often tepid.

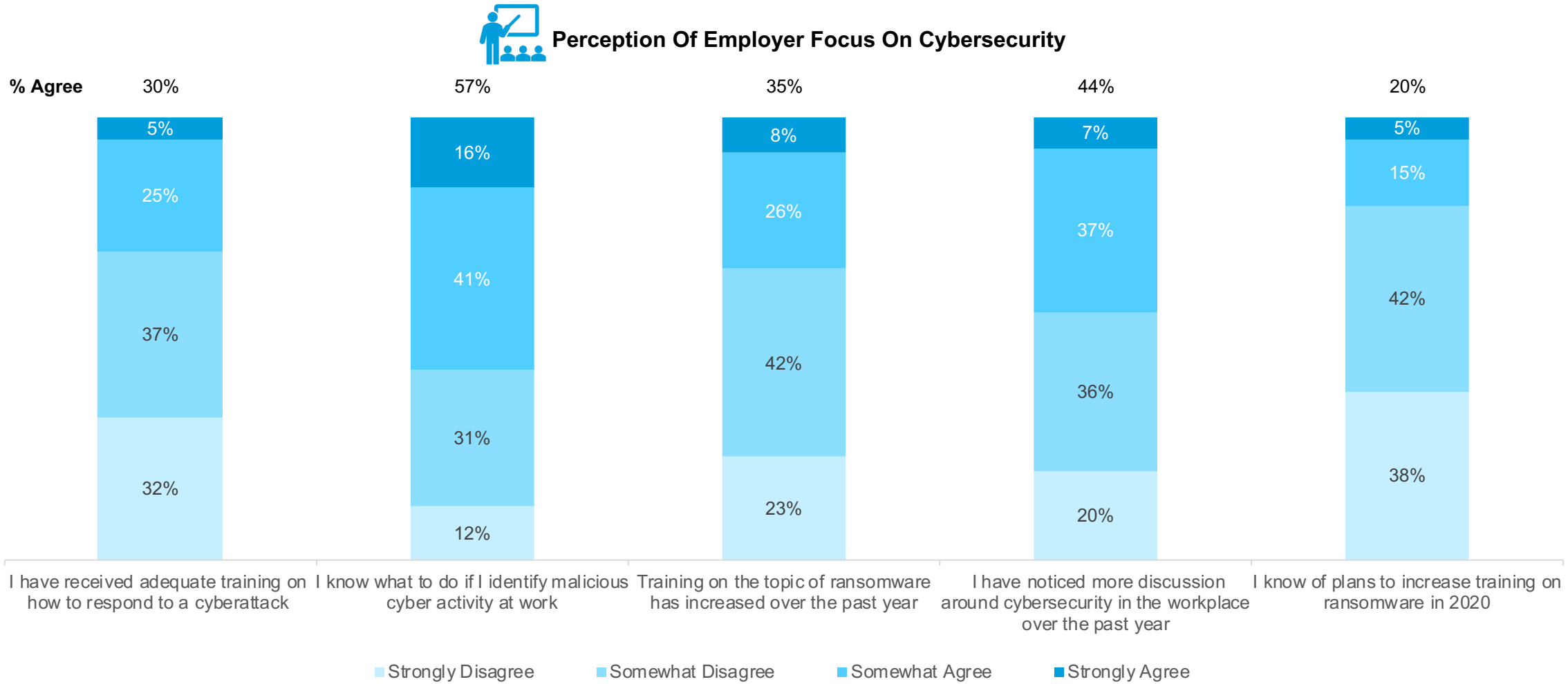
Yet, despite only 49% having received adequate training, most are confident in their own ability to identify a threat.

Perception Of Employer Focus On Cybersecurity



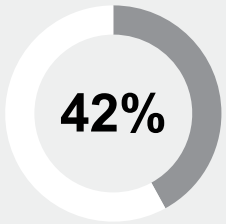
Only three in ten Education employees feel they have adequate cybersecurity training and even less agree that they know of plans to increase training in 2020.

In general, employees in the Education sector receive the least amount of cybersecurity training overall.

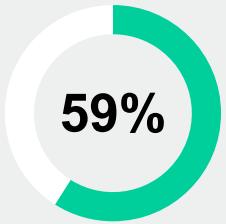


Audience Overview

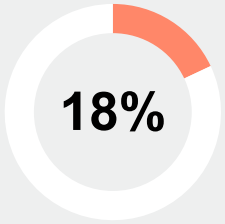
Works For The State Government



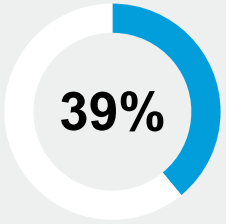
All Employees



IT

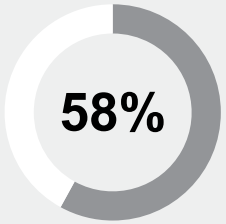


Emergency

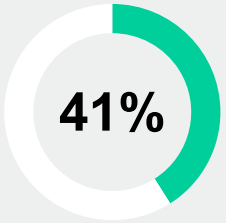


Education

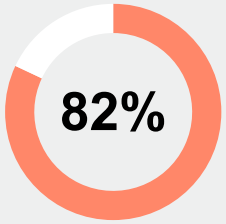
Works For The Local Government



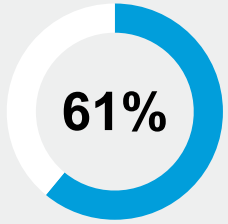
All Employees



IT



Emergency



Education

Local Government Breakdown