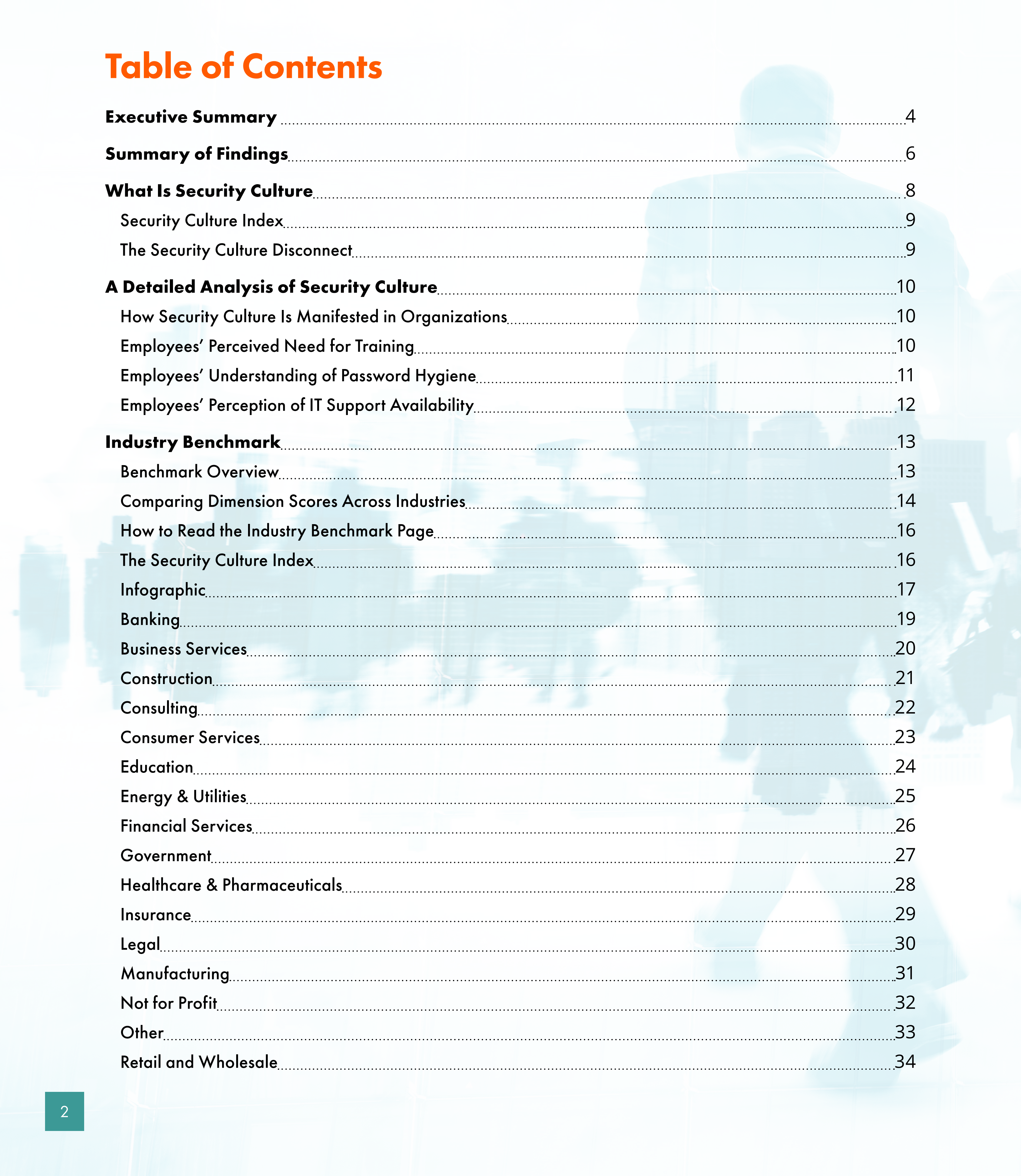
KnowBe4 Research

CLTRe
a KnowBe4 company

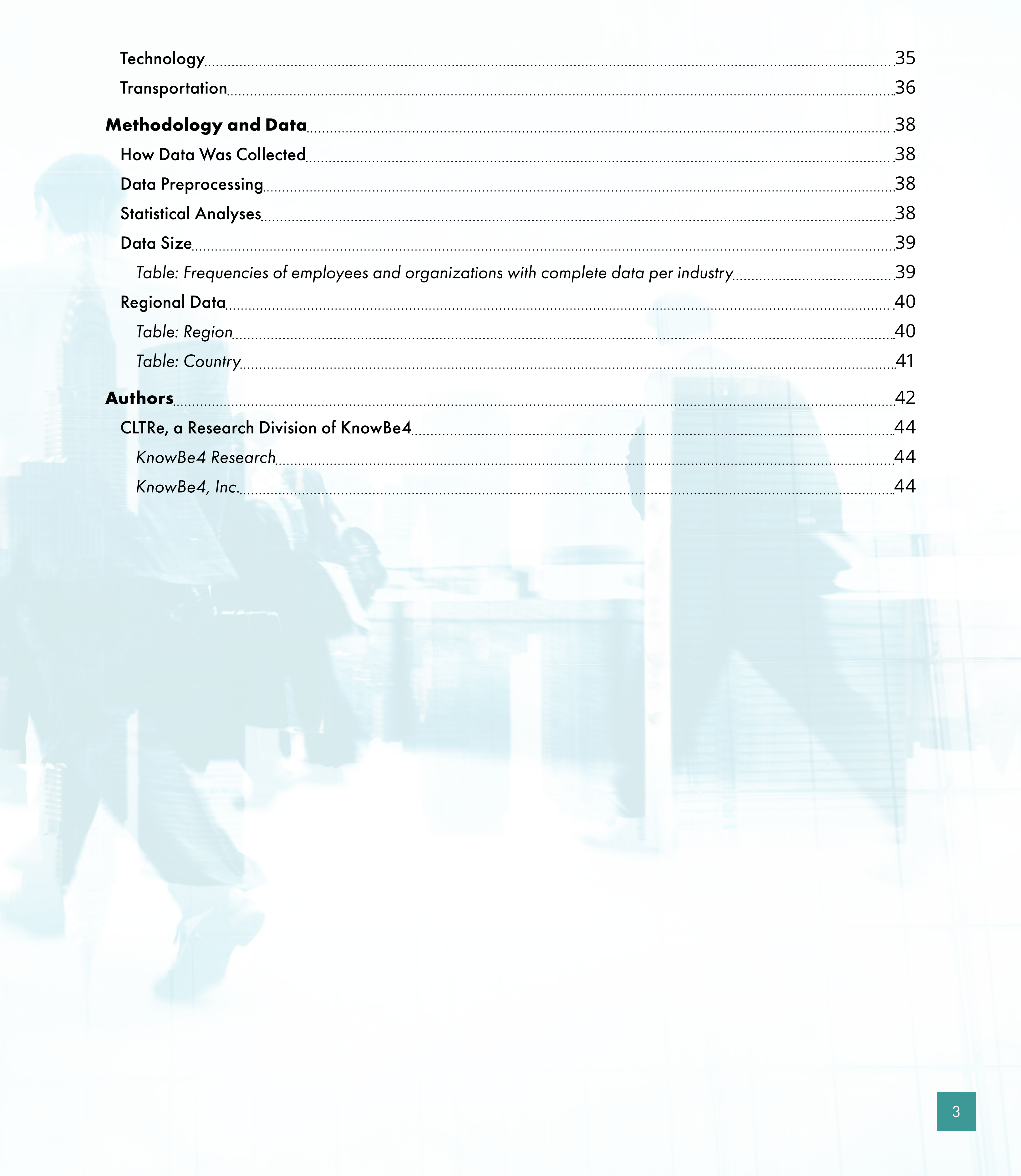
# The Security Culture Report 2021

## A Global Security Culture Perspective During a Pandemic

Anita-Catrin Eriksen
Kai Roer
Dr. Gregor Petrič
Joanna Huisman
Rosa L. Smothers
Perry Carpenter



# Table of Contents



# Executive Summary

Welcome to the 2021 Security Culture Report, the fourth annual report of its kind. The Security Culture Report and associated methodology was originally developed by CLTRe, which was acquired by KnowBe4 in 2019, and is KnowBe4 Research's most ambitious report. The data represented here was collected during the global COVID-19 pandemic and, as such, some findings from our research reflect both positive and negative inflections that may be attributable to pandemic conditions.

Security culture is the ideas, customs and social behaviors of an organization that influence their security. Of 1,161 security leaders surveyed in 2020, 94% reported[1] that security culture is the most important element in their security strategy. This sentiment is reflected in the growth in the number of organizations measuring their security culture.

> More than 94% of security leaders around the world believe that security culture is critical.

More than 320,000 employees, in 1,872 organizations around the world have been surveyed in this largest ever study of security culture. While some industries saw security culture stagnate or decline during the pandemic, we were encouraged to see a number of industries use the pandemic as an opportunity to improve.

[1] The Security Culture Report 2020

Organizations with a poor security culture demonstrate a 52-time higher risk of employees sharing credentials.

Security culture is directly associated with reduced risk. In a recently published KnowBe4 Research report, we demonstrated that organizations with poor security culture have a risk that is 52 times higher for employees sharing credentials.[2] As of yet, there are no industries that quantifiably demonstrate a good security culture, which is characterized by a score of 80 points or more. This is worrying when we see a continued growth in the threat level, and a growing number of victims of cybercrime. According to CoveWare, 2020 saw ransomware payments reach an all-time high with organizations across all industries being targeted. The most common method used by hackers to gain access to their target systems is by social engineering.

In their Q4 2020 Ransomware Marketplace Report, the ransomware remediation and analytics firm CoveWare noted that for the first time, phishing surpassed other techniques as the most common tool[3] used by hackers to gain access. As such, organizations around the world—large and small—should expect to see an increase in phishing attacks in the coming years.

Security culture is a critical, need-to-have asset in the security toolbox. By assessing employees' security awareness, behaviors and culture, organizations can adapt their policies and training programs to the constantly changing threat landscape. The alternative becomes less attractive by the hour: do nothing and see your organization crumble to a halt by ransomware, data theft or business interruption.

[2] Security Culture and Credential Sharing, 2021, KnowBe4 Research

[3] https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020

# Summary of Findings

2020 was heavily influenced by the global effects of COVID-19. And we believe that we see pandemic-related ripples within some of the year-over-year changes detected in security culture. This is a high-level summary of the findings:

## Embracing Digital Transformation:

- The education industry improved by two points. This improvement may be explained by education being moved from classrooms to virtual settings due to the COVID-19 pandemic and the associated technology systems and training changes.
- The legal industry also increased their score by two points. Again, we may explain this improvement by many legal processes and procedures being moved online.

## Suffering from Chaos and Confusion:

On the other side of the spectrum, the news is not so good:

- The Consumer Services industry dropped one point lower this year. This may be due to the reduction in the workforce during the pandemic.
- The Construction industry also scored one point lower than last year. Again, we believe this may be explained by the reduction in workforce due to the pandemic.
- The Business Services also scored one point lower this year. This sector has traditionally shown a high score, making this change somewhat surprising.

Results from this year's report revealed a large gap between the best performers and the poor performers. Unsurprisingly, the best performers were from Financial Services and Banking—industries with a long tradition of managing risk. However, being a "best performer" doesn't necessarily equate to having performed at a desirable level, and these industries shouldn't be too quick to congratulate themselves. For instance, a score of 76, as seen by Banking and Financial Services, is well below a Good security culture. Our research shows that moving from one security culture class to another is directly correlated to risk. By improving from the current class of Moderate to the next class of Good security culture, these industries will see a reduction by eight times of employees sharing credentials.[4]

As in earlier reports, the Education industry is one of the worst performers, with a score of 70. Even though Education is still at the bottom of the list, this industry has shown a significant improvement compared to earlier years and is now demonstrating Moderate security culture. This improvement helps reduce the risk of employees sharing credentials by three times.[4]

Another industry that saw an improvement from last year is the Legal industry, with a new score of 73. This change may be explained by the pandemic forcing many legal and court operations online. Even if some users seem to struggle with the technology[5], the adoption of technology is showing an improved security culture too.

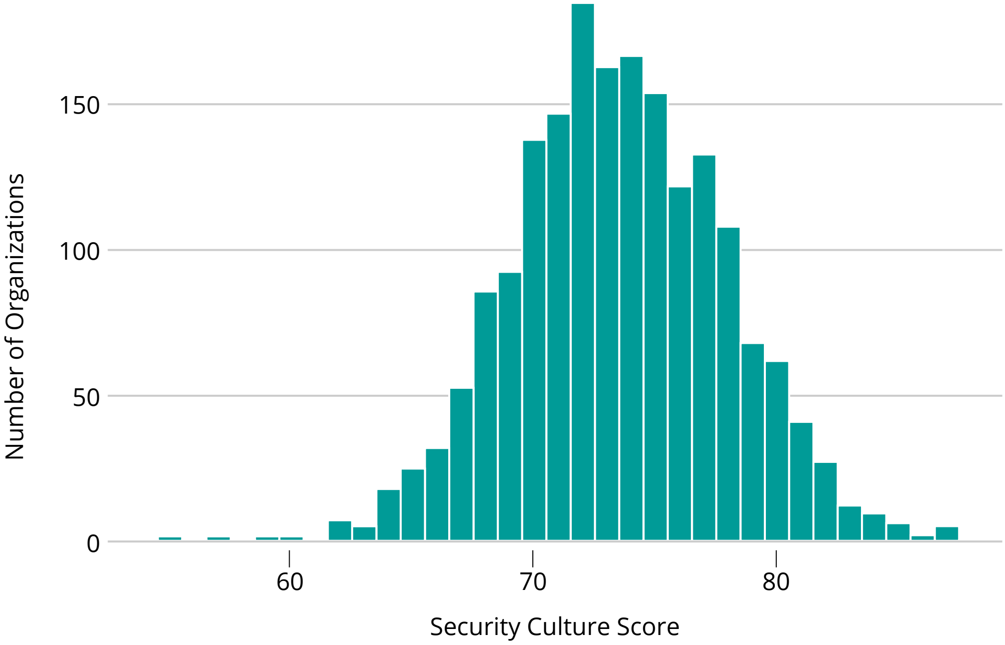
[4] Security Culture and Credential Sharing, 2021, KnowBe4 Research

[5] https://edition.cnn.com/2021/02/10/tech/cat-lawyer-zoom-filter/index.html

Sharing the bottom placement with the Education sector is the Construction industry. Unlike the Education industry, Construction experienced a drop in their security culture during the pandemic. Other industries with a reduction in security culture are the Consumer Services industry, with a new score of 72, and Business Services, with a new score of 74.

In this year's report, we present a deep dive into security culture with the new report section, A Detailed Analysis of Security Culture. This section provides an in-depth view to the state of specific aspects of security culture. We look at how employees consider their sentiments about having access to security-related information, how they think about passwords and their access to the security team.

*Figure: Distribution of Organizations According to Their Security Culture Score*



The mean and median of the total security culture score is 73. Detailed analysis shows that the majority of all analyzed organizations managed to develop a mediocre or moderate security culture, while only a small portion of organizations have a good security culture. Alarmingly, a few organizations are scoring in the Poor bracket and no organizations have reached an Excellent security culture score yet.

# What Is Security Culture

Security culture is the ideas, customs and social behaviors that impact an organization's security. In information security culture, we look at how the cultural aspects influence the information management. In cybersecurity culture, the focus is on the part of information management that uses cyber technology to create, manipulate or store information and data.

The purpose of the security culture survey and the Security Culture Report is to provide an objective scientific method for assessing, reporting and comparing the relative information security culture-related strengths and weaknesses of individuals, organizations, industry sectors, regions and more.

> **Security culture:** The ideas, customs and social behaviors of an organization that influence their security.

## Security Culture Dimensions

We systematically evaluate culture across seven distinct dimensions; they are:

| | |
|---|---|
| **Attitudes** | The feelings and beliefs that employees have toward the security protocols and issues. |
| **Behaviors** | The actions and activities of employees that have direct or indirect impact on the security of the organization. |
| **Cognition** | Employees' understanding, knowledge and awareness of security issues and activities. |
| **Communication** | The quality of communication channels to discuss security-related topics, promote a sense of belonging and provide support for security issues and incident reporting. |
| **Compliance** | The knowledge of written security policies and the extent that employees follow them. |
| **Norms** | The knowledge of and adherence to unwritten rules of conduct in the organization. |
| **Responsibilities** | How employees perceive their role as a critical factor in sustaining or endangering the security of the organization. |

# Security Culture Index

The Security Culture Index is the scale used to measure security culture. Each of the Security Culture Dimensions are given a score, and then the total for all the dimensions is calculated. The mean of the total is the Security Culture Score, which is used to compare each industry and organization against the Security Culture Scale:

| Poor | Mediocre | Moderate | Good | Excellent |
|---|---|---|---|---|
| 0 up to 60 | 60 up to 70 | 70 up to 80 | 80 up to 90 | 90 up to 100 |

# The Security Culture Disconnect

In the 2020 Security Culture Report, we reported a security culture disconnect globally. A large majority of security leaders worldwide reported that security culture is crucial for their security program. We showed that business principles are the main motivation for building a strong security culture. Building business success (49%), business integrity (43%) and a sense of customer security (41%) were security leaders' top motivations for creating a strong security culture. However, we also reported that the same security leaders miss a common definition of security culture. This inability to define security culture leads to an over-confidence for organizations' security cultures. In our report this year, we demonstrate that the overconfidence is shown clearly in how organizations earn security culture scores: not one single industry earned a score of Good security culture.

This lack of understanding security culture introduces a number of challenges for organizations' abilities to build and maintain security cultures.

We define security culture as the ideas, customs and social behaviors of an organization that influence their security. To work with security culture, we must first understand it. It should be clear that to measure and manage culture, we need to apply other tools, techniques and practices than traditional security controls. The Verizon DBIR 2020 identifies phishing as the most common threat action. Research by KnowBe4 clearly demonstrates the value of assessing the phish-proneness of an organization and using that data to tailor training and education to each employee's need.

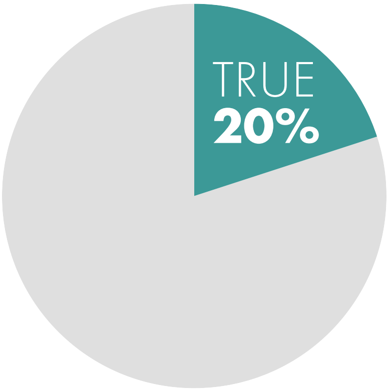
Furthermore, data from KnowBe4 Research shows the immediate role of security culture in lowering employee-induced risks in organizations. See our research paper Security Culture and Credential Sharing, 2021 as an example; in this report, we demonstrate a direct link between the quality of a security culture and the number of employees sharing credentials in a phishing assessment.

# A Detailed Analysis of Security Culture

## How Security Culture Is Manifested in Organizations

In this section, we analyzed data from over 200,000 employees across the world to see how they feel about the information security in their organization. One of the things we are interested in is to learn what a Poor security culture looks like. Why? As mentioned previously, data show that there are great gains to be had by organizations to improve their security culture. For example, organizations with a Poor culture are 52 times more likely to share credentials than those with a Good security culture.[6] By examining how employees report on specific topics, we can help their organization to improve security culture by focusing their efforts where it matters most. Specifically, we looked at how employees report their sentiments about having access to security-related information, how they think about passwords and their access to the security team.

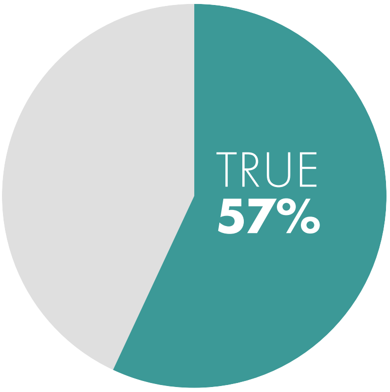
**We do not receive enough training on information security**



## Employees' Perceived Need for Training

Our analysis shows that one in five employees do not feel like they receive enough security information. The potential consequences of this are many. For instance, lack of information could be related to poor understanding of when employees need to report incidents and adhere to security standards. Providing information to employees is a fundamental building block for security behaviors. Given the many tools, resources and strategies created to tackle this specific issue, it is surprising that more organizations are not succeeding in this area. Organizations can leverage online training and ramp up internal employee engagement campaigns to address this issue, giving every employee access to the security information they need.

**I will notice if my computer is compromised**



Our analysis shows that 57% of employees believe that they would recognize if their device got hacked. This is alarming, given that many cybersecurity threats, including ransomware like Ryuk, can go undetected for months before detection by even the best organizations.[7] Employee misperceptions are often consequences of organizations failing to properly train their employees. A proactive security awareness training program and continuous effort to improve security culture will help employees to recognize and address their blind spots.

[6] Security Culture and Credential Sharing, KnowBe4, 2021

[7] https://www.bleepingcomputer.com/news/security/ryuk-ransomware-crew-makes-640-000-in-recent-activity-surge/

# Employees' Understanding of Password Hygiene

The training of employees also impacts their understanding of why passwords are important. Our industry's fast changing rules of what good password hygiene is complicates matters with password understanding. Over the past 30 years, security experts have trained employees to do contradictory things—from change their passwords every 30 days, to no need to change passwords unless they are in a breach; from limiting the number of characters (which interestingly, some services still seem to be doing) to having a minimum number of characters; from using only numbers or letters, to enforcing all kinds of numbers, symbols, letters and cases. It is no wonder why employees find it difficult to know what the rules are.

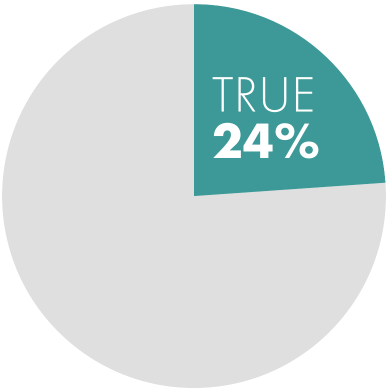
Leaked, breached, shared or cracked passwords are still one of the most important methods for gaining illicit access to computer systems. Criminals have upped their game on social engineering and use a number of different strategies to gain access to what they ultimately want: your money. Earlier, we mentioned ransomware; another big hitter, Business Email Compromise (BEC) attacks, have nearly doubled over the past year according to the Spear Phishing Report 5 from Barracuda.[8]

Our research shows that there is a large gap between what organizations teach, and what their employees internalize when it comes to password hygiene. In our analysis, we see that 24% of employees think that short and simple passwords do not increase the risk of an attack on the organization.

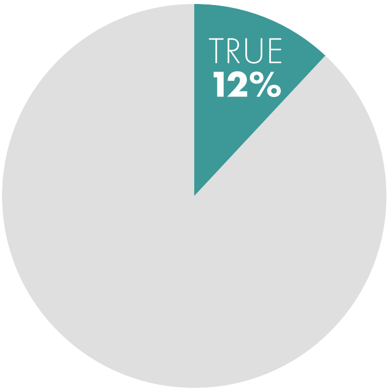
This indicates that employees need more training to understand how weak passwords are a risk to both themselves and their employer. Twelve percent report that they do not understand why it is necessary to change their passwords if only they know it.

In 2020, we continued to see a large amount of data breaches resulting in leaked credentials according to Statista.[9] KnowBe4 data shows that one in four employees reuse their passwords across different services.[10] If your employees do not understand the risk associated with bad password hygiene or the need to change stolen passwords, then training in this area is urgently needed to reduce risk.

**Short and simple passwords are not helping hackers**



**Do not understand why it is important to change passwords**



[8] https://www.barracuda.com/spear-phishing-report-5

[9] https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

[10] https://www.knowbe4.com/breached-password-test

Research by LastPass in 2019[11] claims that at large enterprises, employees have an average of 25 unique logins, and small businesses may have up to 80 unique logins. The number of unique services and logins are likely to be similar, even for the majority of organizations that are not using any password management solution. In our research, we found that 77% of the employees do not use any means to securely store their passwords. The fact that most employees are required to have a large number of logins, while they are not able to save their passwords in a secure location, suggests that most employees reuse passwords.

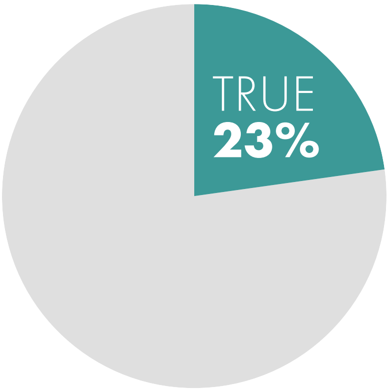
## Employees' Perception of IT Support Availability

One of the most important security measures for organizations should be to ensure all employees know what to do and who to contact in the case of a security incident. Our research shows that 30% of employees report that it is difficult to reach the security experts in their organization. When organizations fail to provide their employees with adequate processes and access to the specialists, a higher number of security breaches are to be expected.

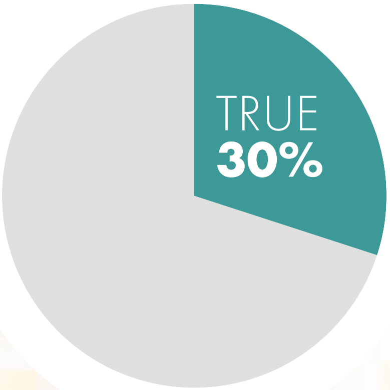
The findings in this section serve as eye openers into how employees around the world report the state of security culture in their organizations. Organizations should take advantage of the relationship between security culture and risk by focusing their efforts on measuring and managing their security culture to ensure they keep improving. We recommend using a standard metric and a de facto benchmark to make it easier to know where your security culture currently stands.

[11] https://www.cpomagazine.com/cyber-security/lastpass-2019-password-security-report-shows-continuing-issues-with-reused-and-stolen-passwords/

**I store (some of) my passwords on my device**



**It is difficult to reach IT-support in our organization**



# Industry Benchmark

In this section, we describe the security culture scores of each industry sector in detail. Use this section to get a deep dive into specific industries, and as a benchmark to compare your own scores against those of different industry sectors.

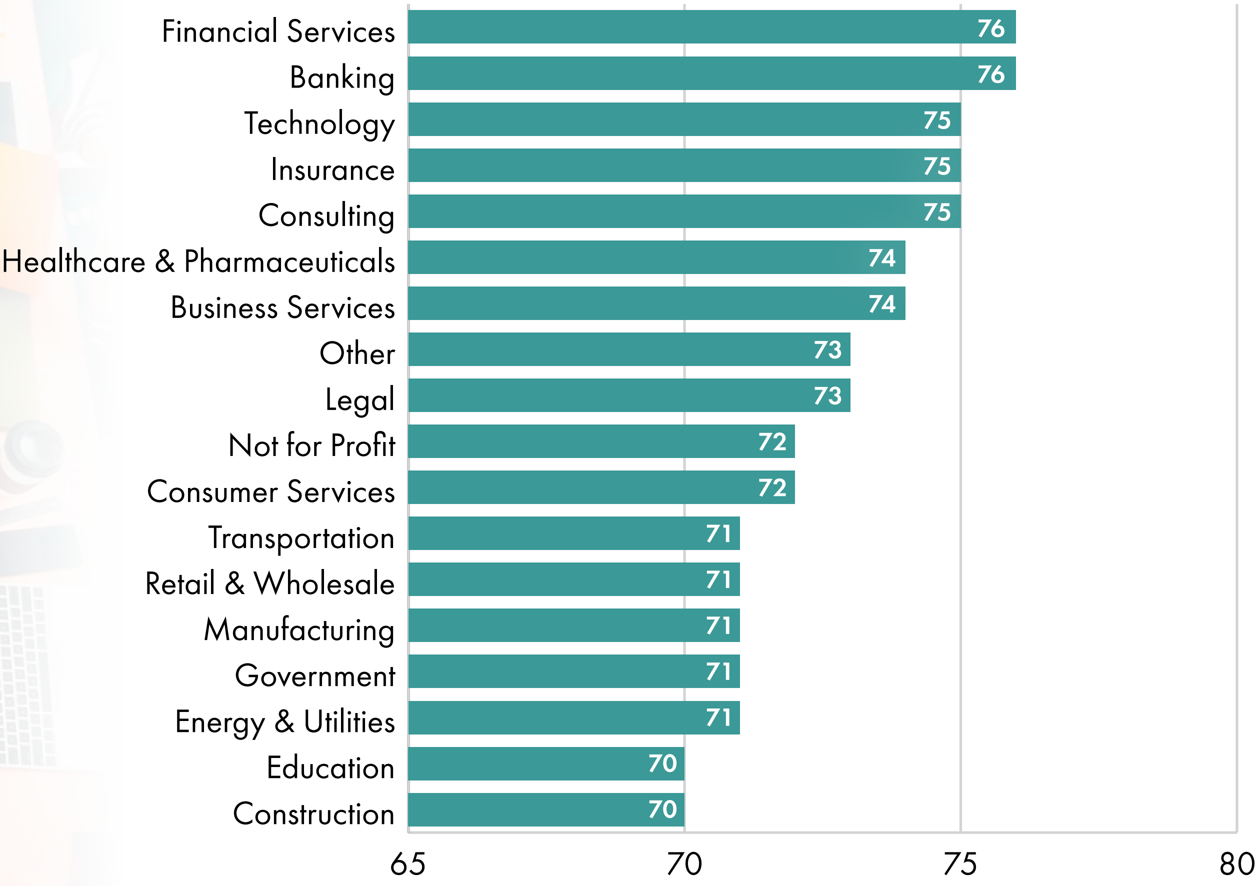
## Benchmark Overview

Security culture varies across industries. In the industry comparison section, we compare all industries according to their security culture scores. We also compare the industries across each of the seven dimensions of security culture.

On these pages, we compare all the industries. This overview provides direct insights into the difference across the industry sectors and it is created to make it easy to understand how your industry compares to the other industries. You can also use this section to compare your organization score with other industry sectors.

### Industry Benchmark

*Figure: Comparing Security Culture Score*

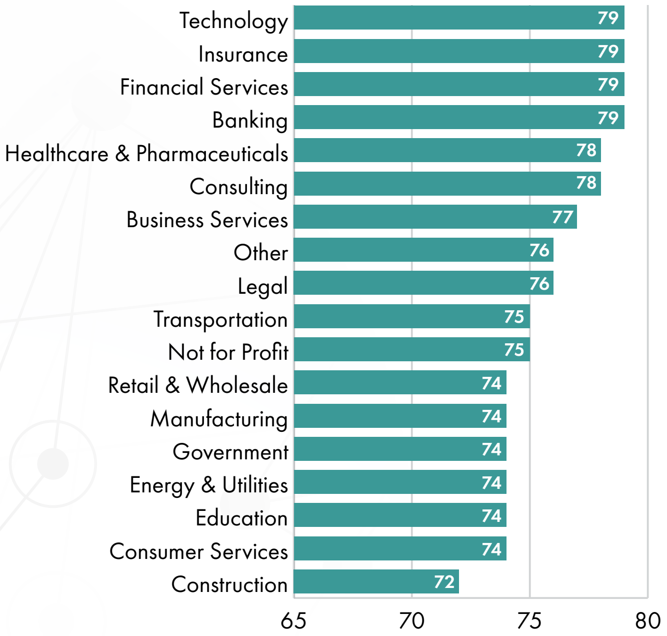


# Comparing Dimension Scores Across Industries

These graphs show how the different industries compare across the seven dimensions of security culture. Use this to understand how each dimension influences each industry.

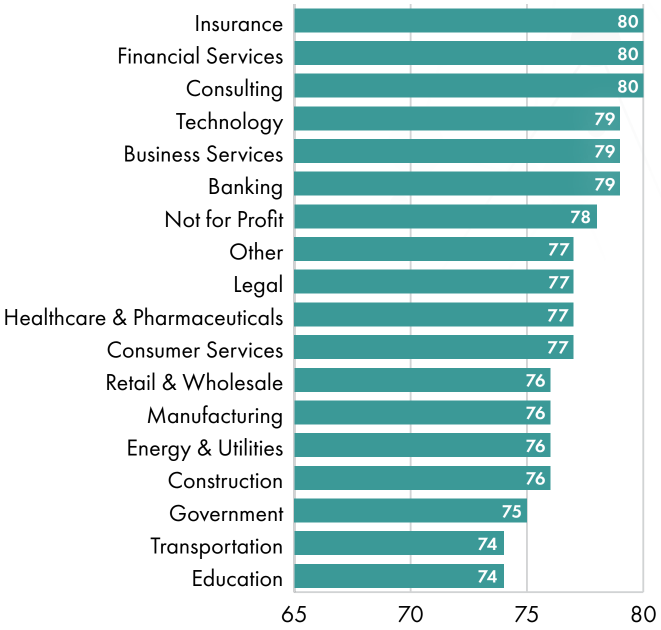
## Attitudes

The feelings and beliefs that employees have toward the security protocols and issues.



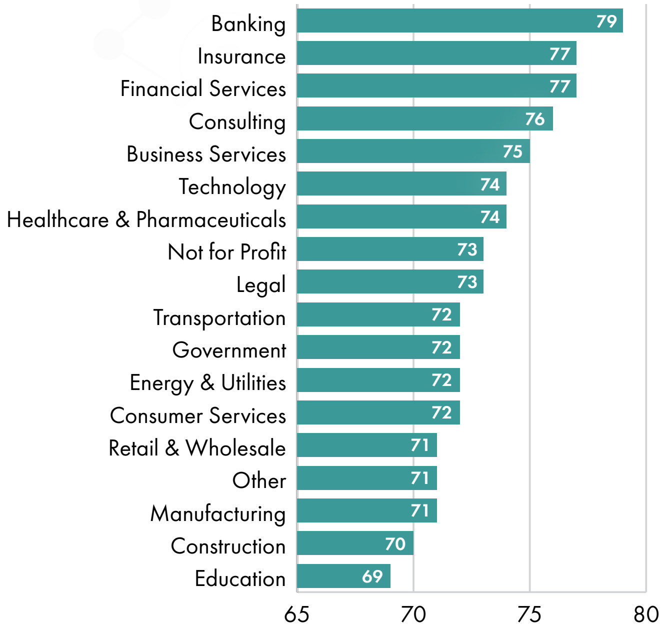
## Communication

The quality of communication channels to discuss security-related topics, promote a sense of belonging and provide support for security issues and incident reporting.



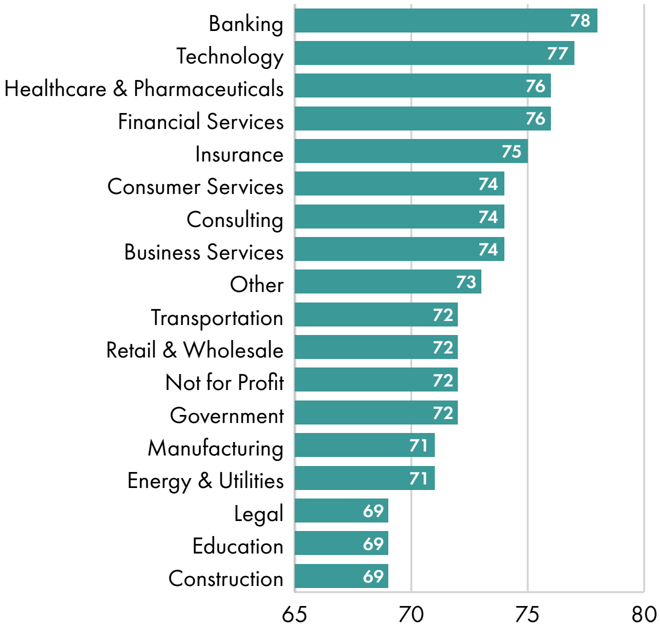
## Compliance

The knowledge of written security policies and the extent that employees follow them.



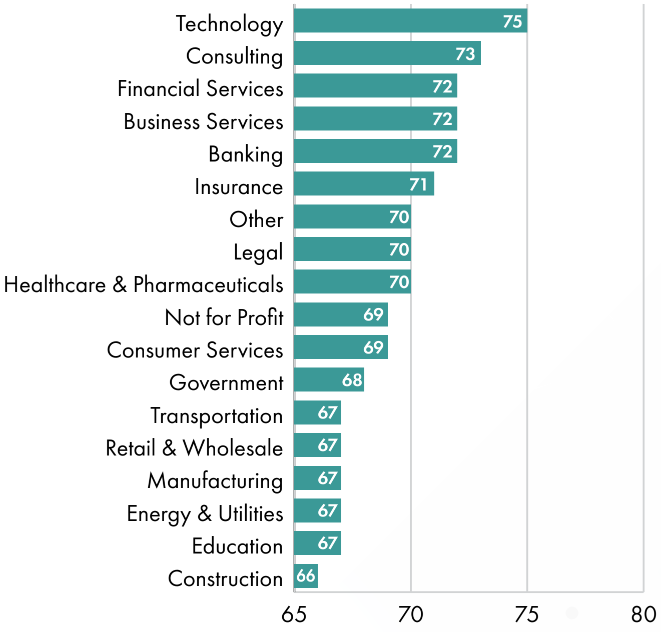
## Behaviors

The actions and activities of employees that have direct or indirect impact on the security of the organization.



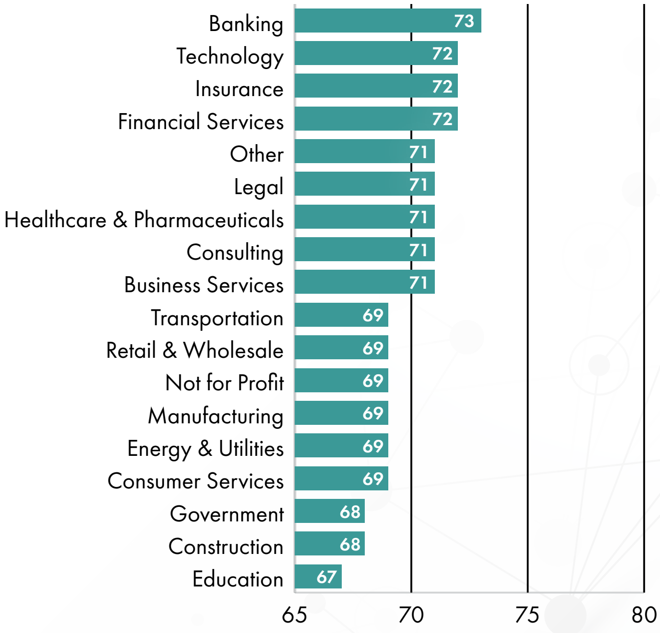
## Cognition

Employees' understanding, knowledge and awareness of security issues and activities.



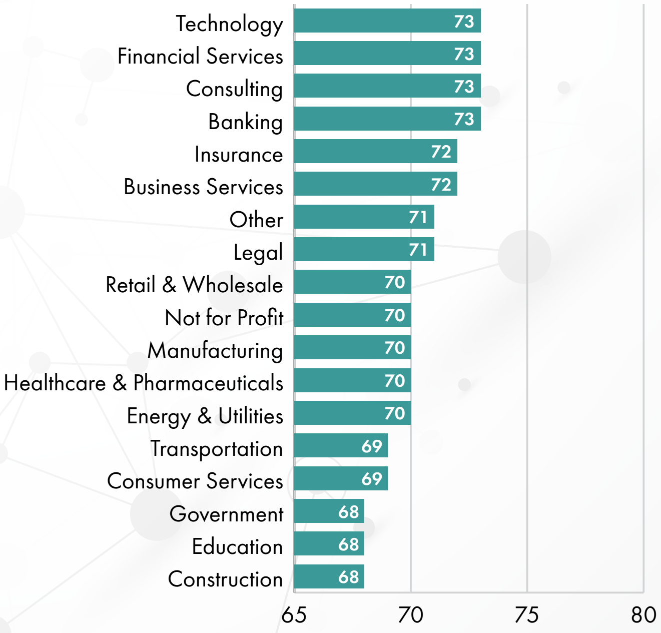
## Norms

The knowledge of and adherence to unwritten rules of conduct in the organization.



## Responsibilities

How employees perceive their role as a critical factor in sustaining or endangering the security of the organization.



# How to Read the Industry Benchmark Page

Each industry sector has its own benchmark. This benchmark includes a description, data points and graphs. Each page is constructed in the same way, with a title, a description, a section on what and how to improve, an overview infographic, a box plot and a column graph. Together, these elements provide a wealth of information, presented in a way to make it easily accessible for any reader. Use the page for your industry to inform yourself, your team and your board of directors on the current state of your industry.

The report uses the Security Culture Index.

## The Security Culture Index

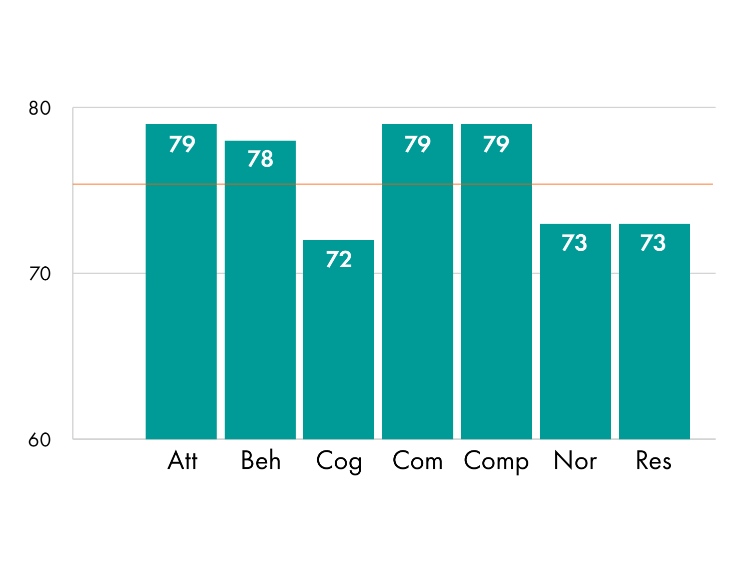
The security culture index is the scale used to understand the security culture score. The scale ranges from 0 (worse) to 100 (best) and uses five levels that explain the quality of the security culture.

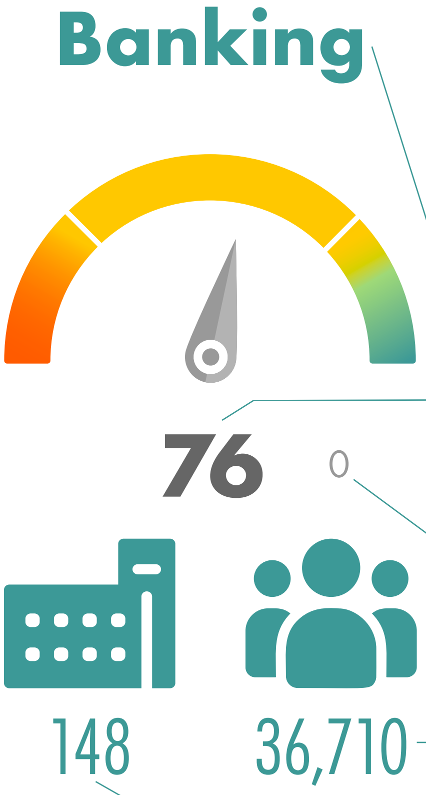
The security culture index levels are:

| | |
|---|---|
| **Excellent** | 90 up to 100 |
| **Good** | 80 up to 90 |
| **Moderate** | 70 up to 80 |
| **Mediocre** | 60 up to 70 |
| **Poor** | 0 up to 60 |

### How to Read the Column Chart

Column charts use columns to compare data. In this report, they are used to compare the seven dimensions of security culture. The height of the bar indicates the score on the dimension. This makes it easy to compare the scores on different dimensions to see where the industry scored the highest, lowest and possibly equally. The bar chart also contains a horizontal line, which indicates the security culture score for the industry. Comparing each column to the line is useful in order to understand the industry´s strong and weak areas.





## Infographic

The infographic is designed to quickly provide you with key data of your industry: The industry name, the industry benchmark score, the number of organizations in the industry and the number of respondents in that industry.

### Industry name

This is the name of the industry as used in this report.

### Industry benchmark score

This is the score for the industry. Use this to compare your own score with that of your peers.

### Change from last year

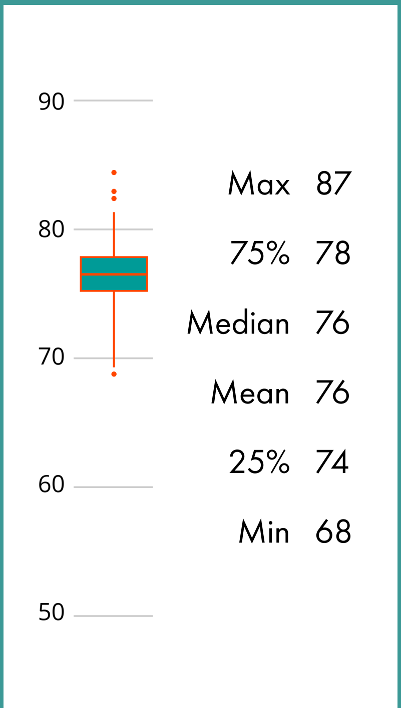
This number shows how your industry benchmark has changed since last time. The number is either 0 (no change), +x (an improvement by x points) or -x (a decline by x points).

### Number of employees

This is the number of employees responding to the survey in this industry.

### Number of organizations

This is the number of organizations in this industry.



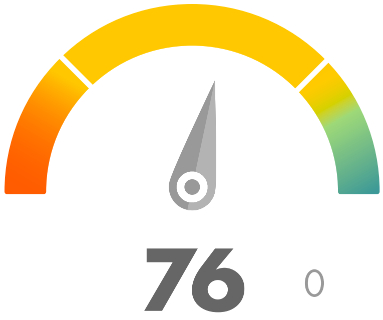
## How to Read the Box Plot

A box plot is a visual representation of important statistics about the data. The box plot is used to easily understand how the data samples are represented across the scale being used. The security culture index uses a scale from 0 to 100, and the box plot visualizes where each organization's security culture score falls within that range.

The line across the center of the plot is the median, which is the middle score of all the scores when they are sorted. The median is enclosed by a box; the start and end point of the box indicates the range within which the middle 50% of all scores fall. There are two lines sticking out from the box. The bottom line indicates where the lower 25% of the scores fall, and the upper line indicates where the top 25% of the scores fall. You might also see some circles on the plot, often referred to as outliers. These scores are very different from the others.

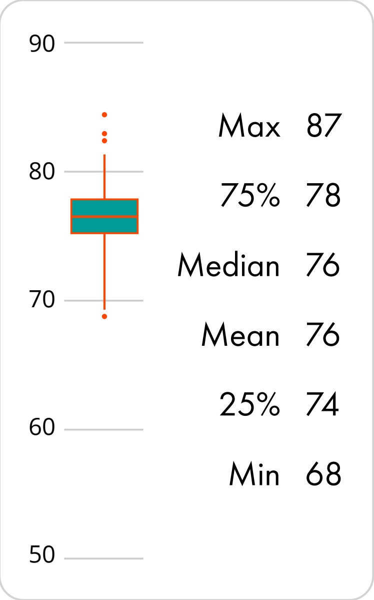
***2020 was heavily influenced by the global effects of COVID-19.*** *And we believe that we see pandemic-related ripples within some of the year-over-year changes detected in security culture.*

# Banking



148

36,710



| | |
|---|---|
| Max | 87 |
| 75% | 78 |
| Median | 76 |
| Mean | 76 |
| 25% | 74 |
| Min | 68 |

Due to the high value of financial data, the Banking sector has long been familiar with risk management concepts. This, often coupled with government-required cybersecurity and employee training standards, drives this industry's overall risk management strategy. The Banking sector's security culture score of 76 is consistent with last year's report.

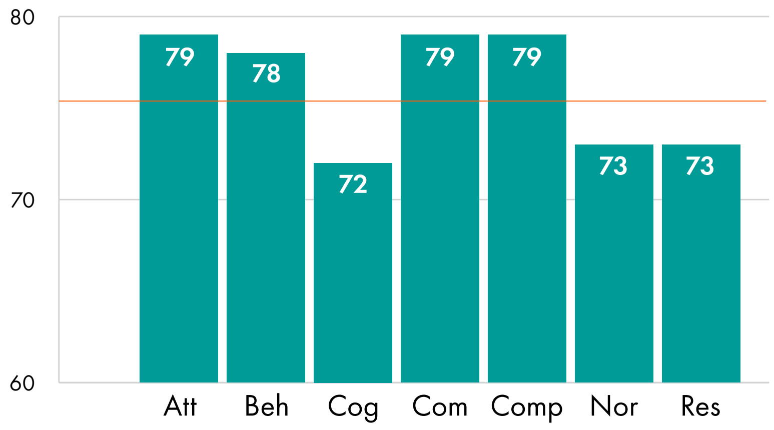
Employee survey results from this sector are also generally consistent with last year, with only minor shifts in some dimensions. With a score of 79 in the Attitudes dimension, a one-point decrease over last year, could be the result of a slight shift in thinking, as the industry grapples with the effects of COVID-19 on day-to-day work, with personnel working in shifts with less face-to-face interaction.

As with the previous year, both the Communication and Compliance dimensions maintained their score of 79. The Banking industry maintains strong communications channels, which serve to enable their employees and an ongoing adherence to industry-specific policies, both of which are vital to security culture. Customers, employees and regulators alike will need specific crisis communication strategies providing assurance that their risk management approach is solid, the financial institution remains secure and that they can continue business without downsizing.

Also consistent with last year's findings are the security Behaviors of Banking industry employees. At 78, the Behaviors dimension reflects this industry's consistent security-based Behaviors. In order to maintain this favorable score, employees will need to anticipate attacks and instinctively understand how to navigate and report them. This will only happen through continuous training and the use of simulated phishing attacks to keep strengthening the security muscle.

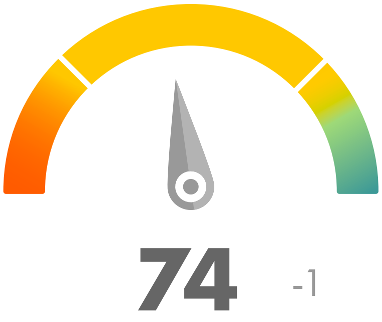
## Areas for Improvement

Moderate scores of 73 in Norms, a one-point increase over last year, a 73 in Responsibilities, also a one-point increase and another 72 in the Cognition dimension, unchanged, provide clear areas of improvement for training and education programs.



Although an improvement of the Norms dimension, which measures the unwritten rules related to security expectations and how employees are adopting them, is a welcome improvement, there is little overall shift in the industry's overall benchmarks. The Banking industry's employees are well accustomed to security training and will likely be highly receptive to a greater emphasis on their responsibilities towards and accounting for security norms.

# Business Services

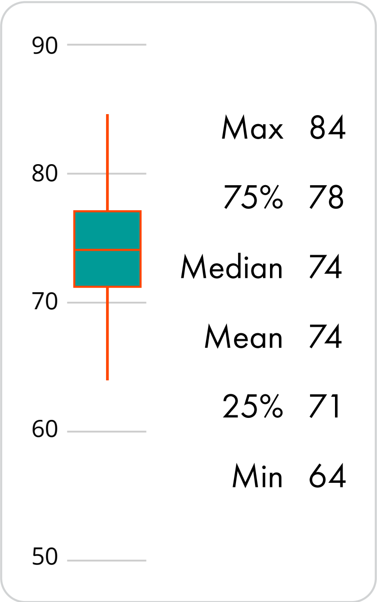


130

12,867

Organizations within the Business Services sector typically offer assistance in areas such as office administration, physical security, garbage disposal, cleaning services and hiring and placing personnel. This sector houses a large variety of organizations offering differing services, making for an interesting mix in overall measurement of descriptive statistics. Historically, this sector has been prone to a high percentage of targeted phishing attacks. Across small, medium and large Business Services organizations, there continues to be a high rate of susceptibility to being compromised, leading to a higher risk level.

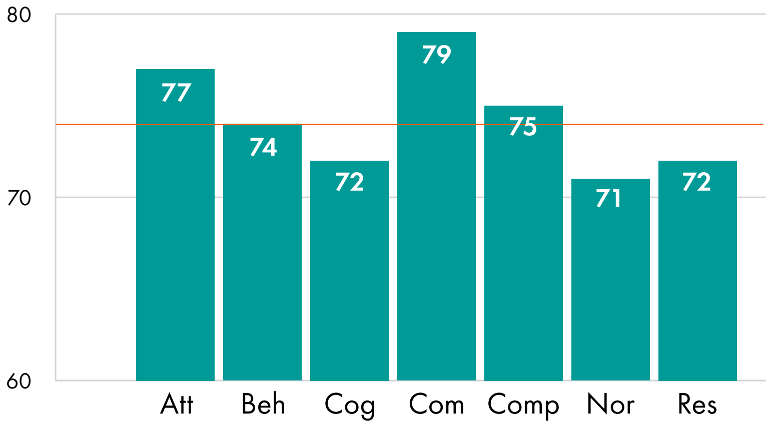
The Business Services sector continues to show a favorably healthy attitude toward security and a willingness to take appropriate measures to better secure their organizations and raise the readiness of their employees, with an overall score of 74. A score of 77 in the Attitudes dimension, a one-point decrease over last year, shows that employees continue to demonstrate a moderate eagerness to be compliant with security measures. Additionally, a good Communication dimension score of 79, also a one-point increase over last year, shows that Business Services organizations are enthusiastic to share security information early and often in their overall efforts to connect with their user population. A consistent year-over-year moderate Compliance score of 75, continues to indicate that Business Services organizations are putting intentional focus on how they communicate, disseminate and reinforce security policies.

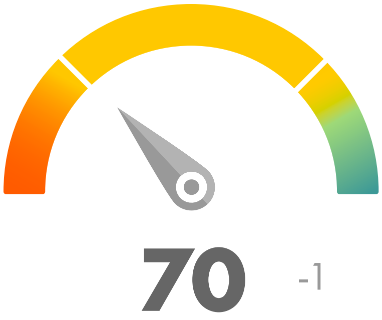


## Areas for Improvement

The Business Services industry has a few clear areas for improvement. With a consistent Cognition score of 72 over last year, we see that although employees demonstrate an eagerness to be compliant with security measures as indicated above, the industry needs to adopt a higher commitment to provide meaningful and ongoing security awareness training for all employees.

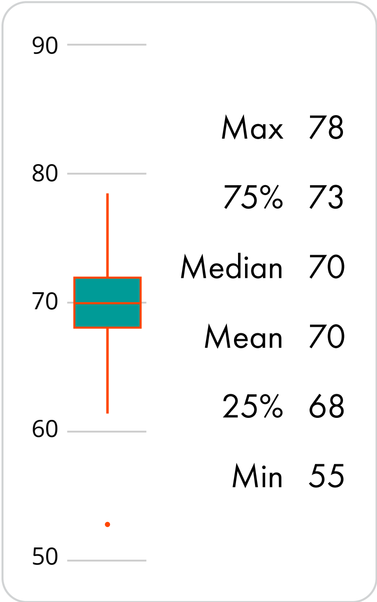
We continue to see more moderate scores of 71 in Norms and 72 in Responsibilities, both unchanged. A strong commitment to comprehensive and continuous training and education will favorably impact these scores. Increased training and awareness, coupled with the already-good communications demonstrated in this industry, will help strengthen employee understanding and buy-in for security-related behaviors and values. Creating a "security champion" (aka culture carrier) program can also be helpful here.





48

6,815



# Construction

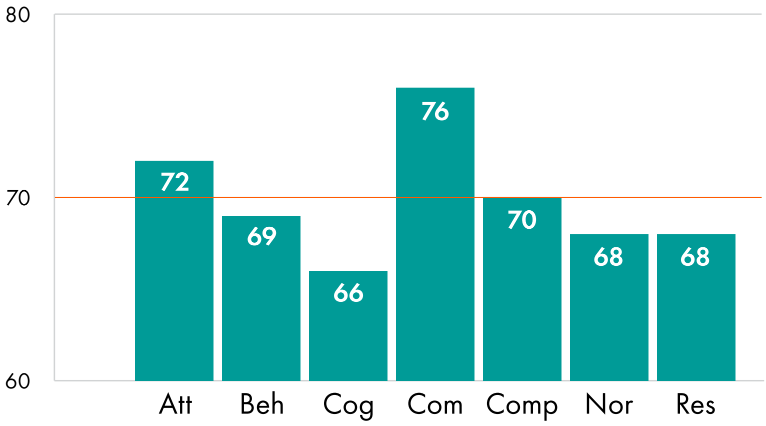
The Construction sector was impacted early by their inability to secure basic materials because of the COVID-19 pandemic. Their overall supply chain was challenged by inflexible architectures and the imminent labor shortages that came soon after. The Construction sector, which often includes a complex chain of contractors, engineers and skilled tradesmen, has long been a healthy target for cybercriminals scoring 70 overall in security culture. The interdependencies associated with this complex structure create even greater complications in the private exchange of information and currency.

The most favorable score for the Construction sector is Communication, a moderate 76, a one-point decrease from last year. This shows that there is a reasonable approach to communicating with employees across their challenging structures. Organizations need to pay close attention to the kinds of messaging being directed at each audience and the mediums through which they communicate. This is a rich environment where cybercriminals thrive. Targeted communications focusing on the unique, security-related threats, issues and responsibilities for each role will help.

## Areas for Improvement

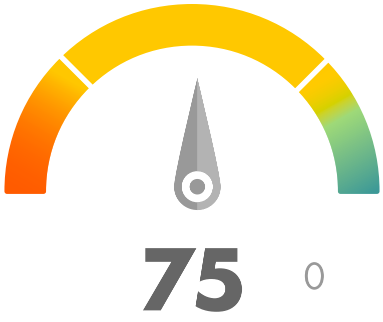
The most significant area for improvement within the Construction sector continues to be Cognition. The score of 66 in this dimension, a one-point decrease from last year, while considered moderate, indicates large gaps in understanding and ownership. A lack of relevant and engaging security awareness training will hinder their ability to become more secure and to evolve their security culture. Many work environments in this industry are not conducive to a traditional computer-based training approach because much of the workforce is widely dispersed on job sites without access to computers and/or centrally managed, handheld devices. This puts an onus on the employees to complete necessary training on their own time or for organizations to slow production to complete training, not a viable option.

The Construction sector is also struggling in the dimensions of Norms at 68, unchanged from last year and Responsibilities at 68, a one-point decrease from last year. Without appropriate mechanisms to deliver necessary security training content, policies and standards, employees are less likely to take ownership of their personal obligation to do their part for the protection of the organization. Employees may mistake unacceptable security-related behaviors as acceptable because there is a lack of understanding of what proper conduct looks like. The Construction industry needs to make time to raise employees' levels of readiness to detect cyber attacks in order to not fall victim to one.



# Consulting

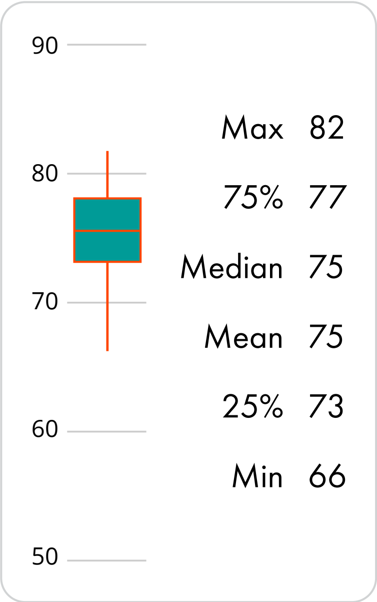
The Consulting sector, with an overall security culture score of 75, remains a very attractive high-profile target for cybercriminals. They are data rich, ranging from intellectual property, financial information, to strategic planning, growth strategies and gap analysis studies. Clients expect elevated levels of confidentiality, which may prove challenging with the high-paced and stressful environment generally bred in this sector. In the era of COVID-19, this sector is likely to see a great deal of disruption in managing current projects and locking in new ones. Specifically, consulting engagements that require onsite collaboration are impacted. This sector will need to find ways to work more efficiently, effectively and securely through different client mediums, while keeping the collaborative spirit alive.



69

5,975

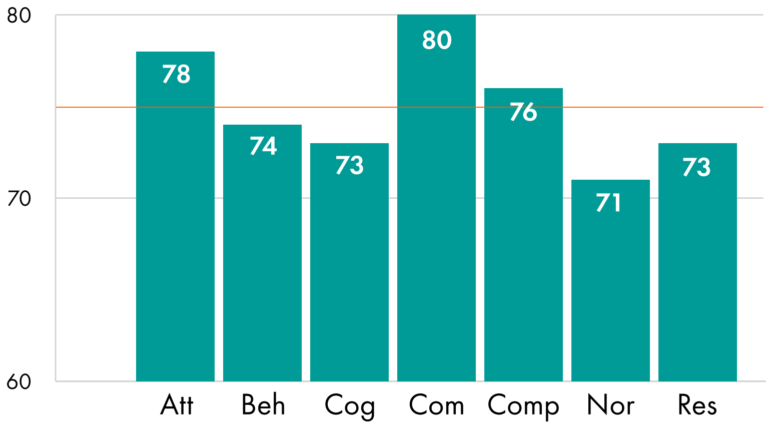
Employees of these organizations demand ready access to information when they need it. But they face a balancing act between providing that access through reliable and secure means to minimize exposure to possible threats versus allowing company data to be shared in an open trough for all employees to feed from. The ability to use communication tools and mediums effectively and efficiently can be the determining factor in preparing the workforce to detect and prevent attacks.



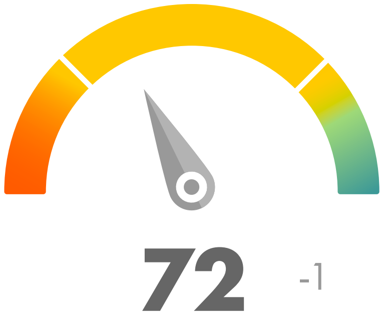
Consulting firms continue to show very positive trends towards becoming more secure through Attitudes at 78, unchanged from last year and Communication at 80, a one-point increase from last year, both on the higher end. With Communication being a cornerstone in the Consulting sector, it is likely that employees understand their respective roles and responsibilities and will readily make appropriate adjustments to adopt more favorable security practices. Additionally, their moderately high score in the Communication dimension, will benefit them during these challenging times.

## Areas for Improvement

With a Cognition score of 73, a one-point increase from last year, it is likely that employees possess an adequate understanding of what their roles and responsibilities are regarding driving a more secure culture. Therefore, security awareness content, delivered in a continuous and relevant manner, is paramount to conveying the required information. Additionally, the score of 71 for Norms, a one-point decrease from last year, is moderately low, revealing that Consulting firms need to continue to use their Communications strengths to define and share these unwritten rules. "The task of building a security culture is thus to stimulate development of norms that support organizational security and ensure these norms become internalized."[1]

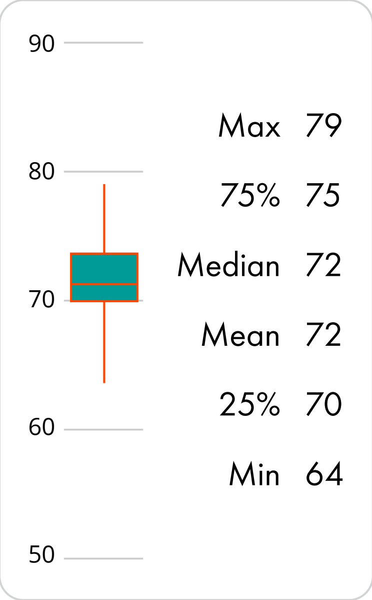


[1] The 7 Dimensions of Security Culture



35

4,986



| | |
|---|---|
| Max | 79 |
| 75% | 75 |
| Median | 72 |
| Mean | 72 |
| 25% | 70 |
| Min | 64 |

# Consumer Services

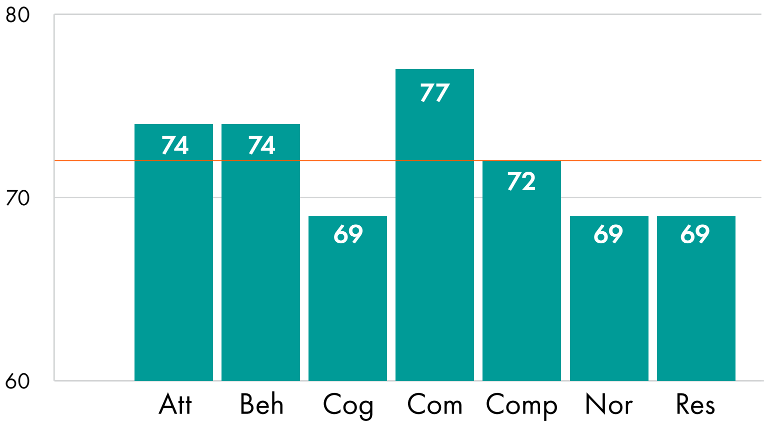
Organizations in the Consumer Services sector typically offer support-based products that are not physical in nature, making for an interesting mix in overall measurement of descriptive statistics. The Consumer Services sector, with an overall security culture score of 72, has long been challenged with keeping up with technological advances that would help to reinforce their security infrastructures; add the global COVID-19 pandemic to the mix, and those deficiencies are magnified. Trying to manage the physical and cyber safety of their employees and customers, coupled with managing a workforce that may now be remote, will prove to be a significant test of their ability to re-examine and adapt to new ways of doing business.

With moderately high scores in the Communication dimension at 77, a one-point increase from last year, we understand that Consumer Services organizations can use communications internally to positively shift the attitudes of their employees and externally to drive trust and confidence through their customer base. Although the Attitude dimension at a 74, was down two points from last year, we know "behavioral security research shows that attitudes are an important predictor of end-user behaviors and can at the same time be influenced by various mechanisms" (Source: The 7 Dimensions of Security Culture).

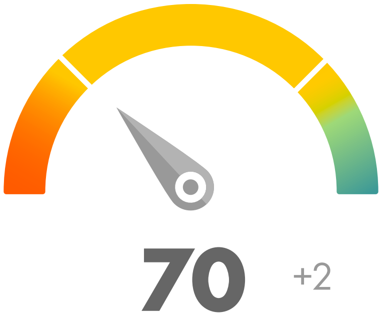
## Areas for Improvement

The dimension of Cognition had a moderate score of 69, unchanged from last year. With a more dispersed pool of talent, Consumer Services organizations are challenged to ensure that there is consistent security understanding across their employees, especially in a more prominent work-from-home (WFH) environment. Questions on whether the ability of currently leveraged technology is able to support growing WFH populations are paramount. As WFH communities are expanded, security protocols need to be adjusted and a re-evaluation of employee readiness needs to be tested.

Two additional dimensions that reflected low moderate scores of 69 were Norms and Responsibilities, both down two points from last year. Consumer Services sector organizations are struggling to establish solid norms due to their diverse and even more disconnected talent pool. If employees struggle with internalizing the unwritten rules, then their ability to connect those rules to what they are personally responsible for in driving a stronger, more defined security culture may be blurred. And as employees are spending less time in the workplace, it is more challenging to reinforce.



# Education

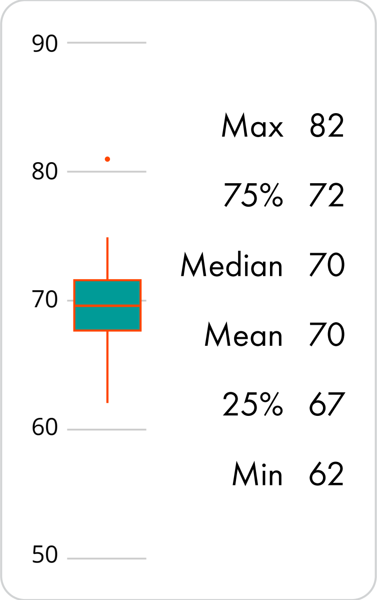


62

8,590

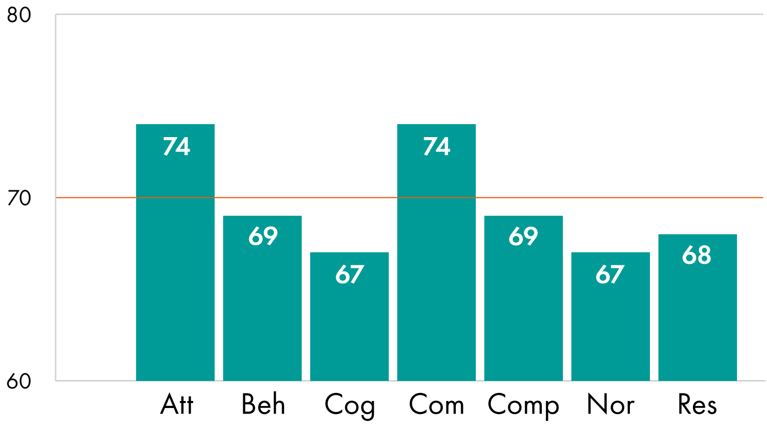
The Education sector has had an especially difficult time due to the COVID-19 pandemic. In addition to the ongoing challenges of a broad variety of institutions (public, private and higher education), the sudden transition of most schools to online or hybrid teaching environments, a shift in "tools of the trade" and an emphasis on remote learning has created a seismic shift in the industry. Despite most institutions facing issues related to limited funding, there is a commendable slight upturn this year in every dimension within the Education sector. The improved security culture score of 70, a two-point increase from last year, falls in the moderate range.

The Education sector continues to indicate a moderate, though slightly improved, attitude toward security. Every dimension indicates an improvement ranging from one to three points. The dimensions of Attitudes, Cognition, Communication, Norms and Responsibilities have increased one point while Compliance and Behaviors have increased by two and three points, respectively. This broad scope of incremental improvement can be attributed to the dramatic shift in work culture and norms associated with the move to online and hybrid learning environments, motivating the industry at large to pay particular attention to security behaviors.

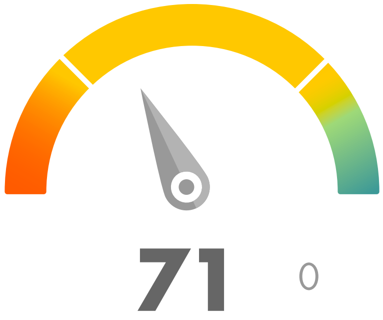


## Areas for Improvement

Last year's assessment found Education in last place ranking in each of our industry comparisons. The broad improvements in security culture are laudatory and these improvements are steps in the right direction for the Education industry. Educational institutions at all levels, but primarily K-12, will need to determine if abbreviated school days, networks that are potentially not secure and at home distractions play a role in security risk on a broader level. Continued focus on all dimensions will help increase their overall security culture, particularly as remote and hybrid school environments will remain in place for the foreseeable future.



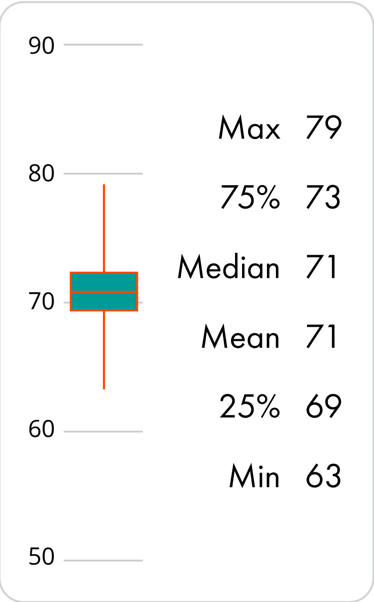
# Energy & Utilities



69 10,129

The Energy & Utilities sector relies upon a series of unique interdependencies between their physical and cyber infrastructures, making companies more potentially vulnerable to exploitation by foreign intelligence services and cybercriminals. Entities such as the U.S. federal government's Cybersecurity Risk Information Sharing Program (CRISP), help provide situational awareness and information sharing in a public-private partnership, enable this sector access to training and materials to identify and address the severity of security risks. Although many such organizations are available to support training and awareness, their industry survey remains steadfast at a moderate security culture score of 71.

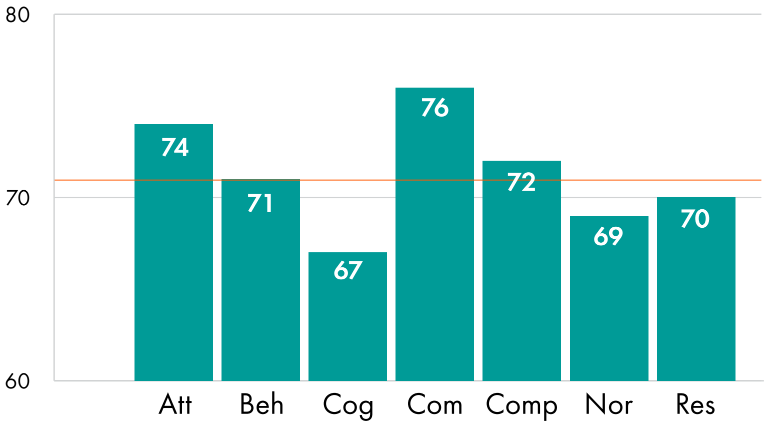
Five of seven dimensions measured showed incremental improvements, most notably Behaviors (71) and Compliance (72), which both increased, indicating that employees are better informed of the impact of their behaviors on overall security culture as well as how to adhere to their industry's compliance policies. Cognition (67), Norms (69) and Responsibilities (70) all increased by one point. These three dimensions are the lowest rated of the seven dimensions and though improvements are evident, additional emphasis in the industry's security programs would benefit any organization.



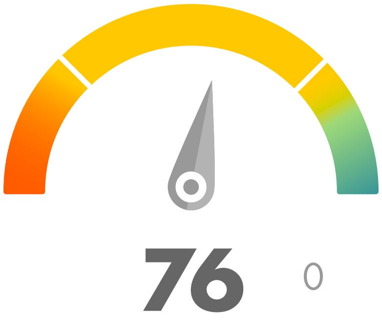
## Areas for Improvement

As with the overall score, two dimensions also remain consistent—Attitudes (74) and Communications (76). All remaining dimensions show incremental improvements. With these steadfast scores, it is apparent that both dimensions can improve both their willingness to implement and maintain security practices as well as how the industry provides pertinent information to their employees.

The Energy & Utilities sector needs to adopt an ultra-diligent focus on ensuring their employees are able to spot an attack and report it. In KnowBe4's Phishing by Industry 2021 Benchmark Report (not yet published), we found that this sector had the highest Phish-Prone™ percentage, employee susceptibility to phishing attacks, in mid-size organizations (250-1,000 employees) at both 90 days and one year after training. It is not enough to just provide training. Employees need to be continuously given opportunities to test their knowledge and learn what to look for should they misstep. A more continuous approach of learning and testing would serve this sector well.



# Financial Services

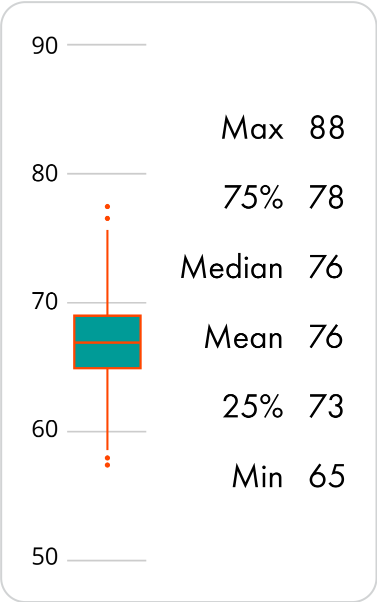


261

32,299

The Financial Services sector is no stranger to risk mitigation practices. When someone controls, trades and governs significant amounts of money, all while housing highly confidential financial and personal client information, it is a given that they would be at the top of a cyber criminal's target list. And, as many companies in the sector move to a more remote work environment, the safety of normal business functions is under a great deal of scrutiny. These organizations may not be able to minimize the number of cyber attacks launched against them, but they can minimize their likelihood of falling victim to one of those attacks; and they seek to do so by adopting a robust, multi-layered defensive strategy and immersing their employees in comprehensive and continuous security awareness training. As a result, their overall security culture score is a moderate 76.

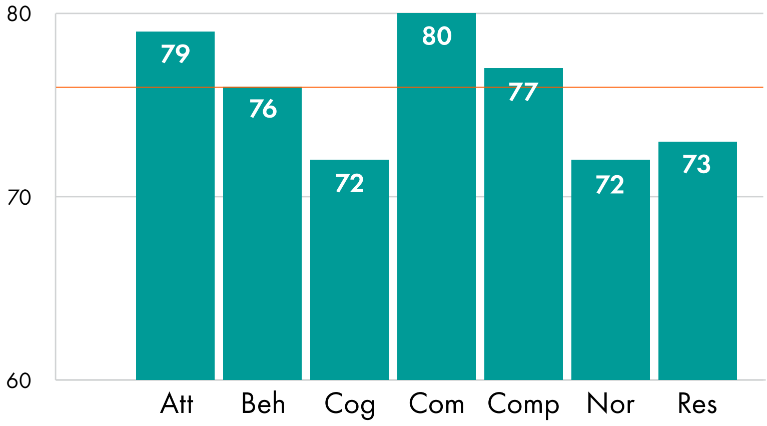
For a second year, the Communication dimension for Financial Services organizations scored in the good category at 80. Threats are quickly evolving in this sector. Pandemic-related market volatility will also play a role in lessened customer engagement and lower confidence in investments.

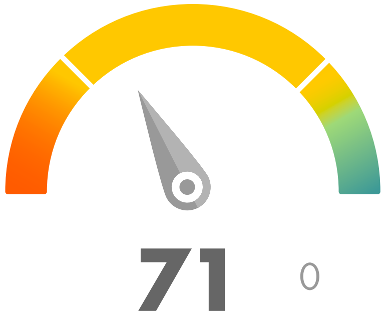


## Areas for Improvement

The Financial Services sector earned a moderate performance score of 72 in the Cognition dimension, unchanged from last year. Employee error is one of the leading security issues facing Financial Services organizations. Consider that "if a person is not aware of basic concepts of information security, he or she is more prone to information security threats than others. Thus, knowledge is one of the key concepts in the research of human factor in information security, and it is a dominant component of information security awareness" (Source: The 7 Dimensions of Security Culture). Adding additional pressure is the threat of personal distraction in the home workplace. Cybercriminals are betting on less training, lower comprehension levels, and for employees to be distracted, not paying attention to what they are clicking on.

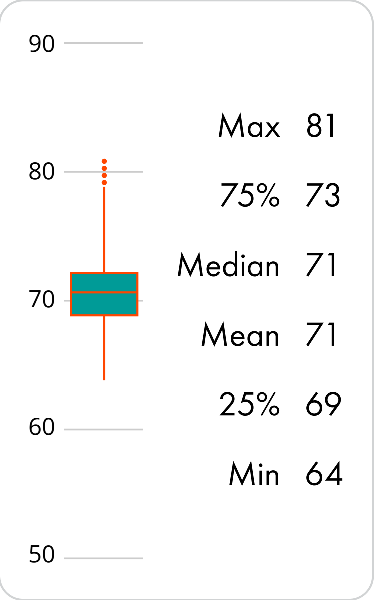
We also recorded a moderate score in the dimension of Norms, 72, a one-point decrease from last year. This score in the Norms dimension is a clear indicator that while time is being spent on training in order to lift understanding, equal time needs to be invested in stimulating professional norms to help drive a stronger security culture and shared values.





133

30,951



# Government

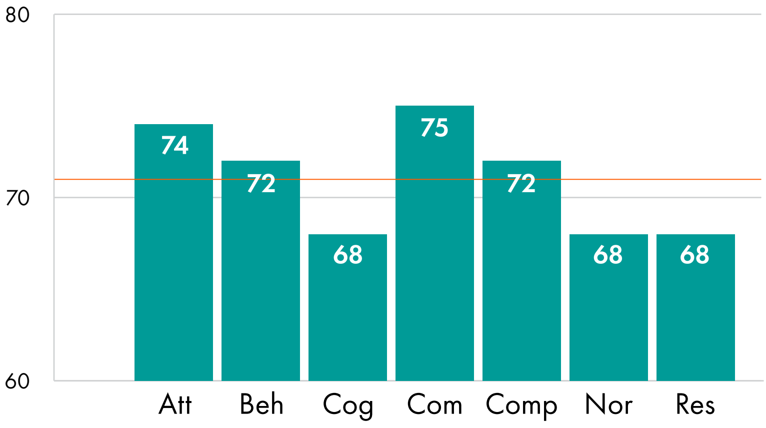
Federal, state and local governments possess broad degrees of experience managing risk on-premise and an increasingly cloud-based infrastructure. The federal government utilizes the National Institute of Standards and Technology (NIST) Cybersecurity Framework and, in addition, the Department of Defense recently released the Cybersecurity Maturity Model Certification (CMMC), which is a new certification procedure used to assess the cybersecurity environment of contracted (vendor) companies. These criteria range from Access Control and Security Awareness to System and Information Integrity. Despite these increased efforts, this sector earned only a moderate security culture score of 71.

Four dimensions of security training remained consistent with last year's scoring: Attitudes, Behaviors, Communication and Compliance. Communication towards security remained the highest score at 75, followed closely by Attitudes at 74 and both Behaviors and Compliance at 72. These consistencies indicate moderate awareness of sanctioned communications resources and the need for situational and security awareness, as well as compliance as it relates to government policies (likely related to issues ranging from password integrity to clean desk policy).

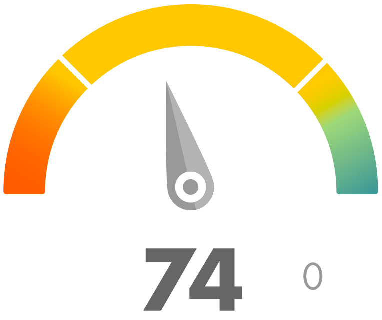
## Areas for Improvement

Government sector organizations continue to exhibit a questionable understanding of security and cybersecurity risks. Though a steady rating, the Compliance score of 72, unchanged from 2020, continues to indicate that employees are in need of additional training as it relates to compliance requirements throughout their sphere of responsibility. There is an ongoing opportunity for improvement in this area.

Most concerning are the low scores of Cognition, Norms and Responsibilities. Cognition increased one point to 68, however this score is still unfortunately low, which indicates a heightened focus on security awareness training is needed as well as a better understanding of how their cyber hygiene affects government's overall security posture. The highly publicized SolarWinds hack may serve to prompt government employees to keep in mind direct as well as supply chain security issues. Cognition's score, combined with declines of Norms and Responsibilities at 68, both one point decreases from last year, highlights the need for the Government workforce to better understand their organization's unwritten rules and codes of conduct, the adoption of that conduct and their sense of ownership of securing their organization.



# Healthcare & Pharmaceuticals



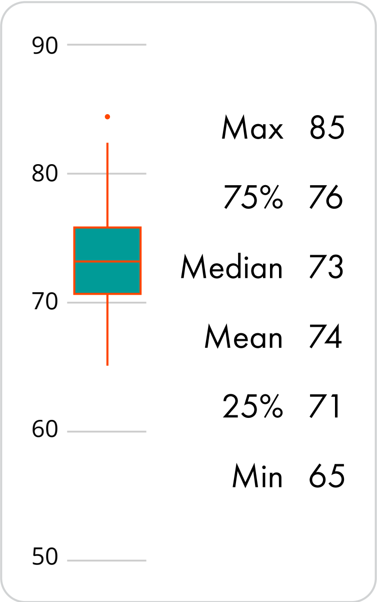
123

17,725

Due to the sensitivities of personally identifiable information (PII) as well as legal requirements such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Healthcare and Pharmaceuticals sector has necessarily demonstrated a broad awareness of the need for security culture. The COVID-19 pandemic has especially impacted how the industry functions, with the increased adoption of telehealth and remote patient monitoring.

Bad actors, motivated by reasons ranging from financial to vaccine development-related espionage, have pivoted their targeting efforts to the remote worker as employees increasingly accessed corporate networks with personal devices. This change combined with the industry's deep understanding of risk management has produced mixed results for the Healthcare and Pharmaceuticals sector's metrics.

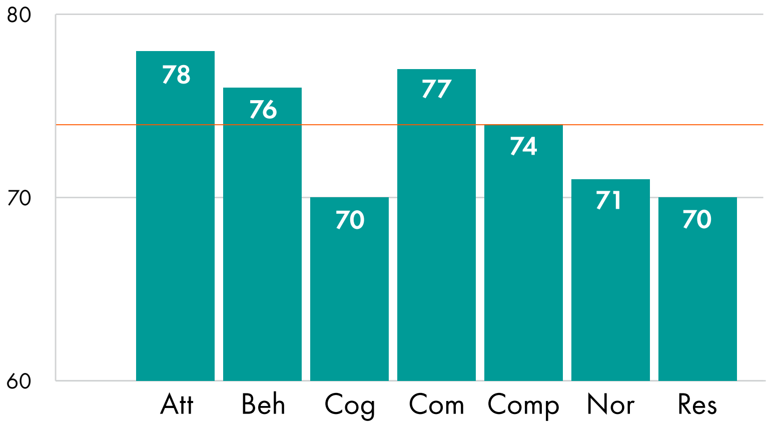
The industry's overall results remain consistent with last year's moderate security culture score of 74 and also maintains its positive attitude toward security culture with a high moderate score of 78 in the Attitudes dimension, unchanged from last year. Also consistent with last year's scores were Cognition (70), Communication (77) and Compliance (74), which indicate employees' ongoing awareness of their security role, their effective means of quickly and securely disseminating relevant information to employees as needed as well as industry-specific policies.



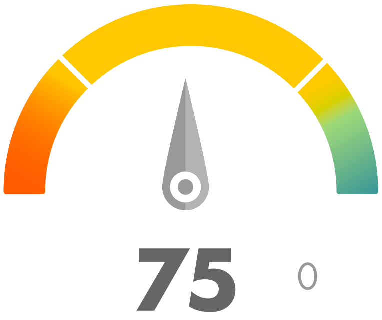
## Areas for Improvement

As with last year's reporting, the Healthcare and Pharmaceuticals sector demonstrates some room for improvement on the Norms dimension which dropped one point to 71. This dimension measures an organization's security-related unwritten rules and acceptable behaviors, and how those are reflected in the actions and values of employees. Employee familiarity and aptitude are vital in the growth of any risk management and training program. Similarly, the Responsibilities dimension also dropped one point to 70. This dimension measures an employee's understanding of the safeguards they provide as those safeguards relate to their organization's security posture.

As with last year, the Cognition score of 70, though consistent, provides another opportunity for potential improvement. The ongoing COVID-19 pandemic has brought not before seen advances (such as the speed to get vaccines FDA approved and ready for distribution), accompanied by serious challenges related to security, supply chain and logistics. Employees in this sector will need to be closely tuned into security issues and activities, and instinctively understand what to do not to fall victim.

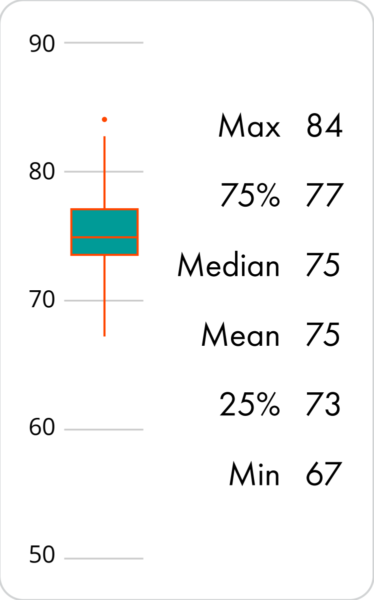


# Insurance



65

15,058



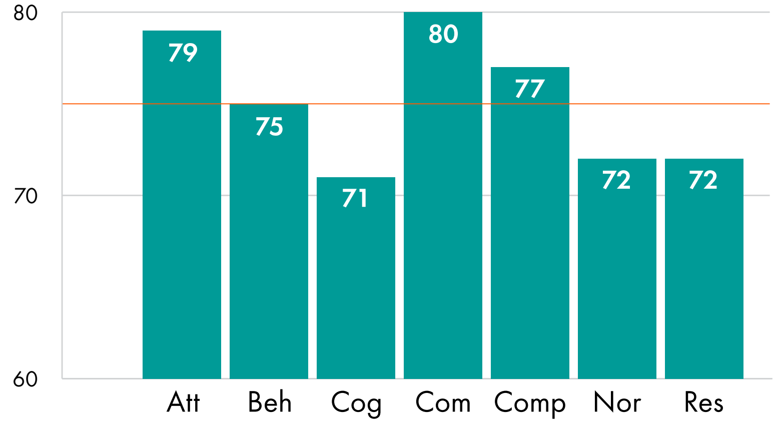
The Insurance sector is a tremendous target for cybercriminals due to the amount of personal, financial and medical information these organizations hold. They are also dealt regulatory fines if they do not adhere to or fall behind on their respective security protocols. In the COVID-19 era, insurers are facing long-term effects. Insurers are looking at potential general liability claims and claims filed against C-level executives, for failure to protect their employees from contracting the virus and not providing a safe working environment. Additionally, insurers that cover travel and events are seeing a record number of cancellations, moving to more virtual conference environments, causing a significant swell of larger dollar claims.

The Insurance sector with an overall security culture score of a moderate 75, showed good attitudes toward Communication, which scored 80, a one-point increase from last year. The need for strong, clear internal and external communications is paramount. Employees need to have accurate and timely information to respond to policyholders in order to promote assurance in their business transactions. They need to be able to convey a level of trust and confidence that keeps business intact.

With a score of 79 in the dimension of Attitudes, a one-point increase from last year, we see that employees within the Insurance sector have good feelings and beliefs related to the importance of their roles in security protocols and issues. A highly regulated industry, insurers need to make certain that they are meeting regulatory standards at every intersection.

## Areas for Improvement

The Insurance sector earned low-moderate performance in the dimension of Cognition at a 71, unchanged from 2020. The Cognition dimension score indicates an immediate need for enhanced and continuous security awareness training that extends to every level of employee, from executives to the front line, to third-party partners. Being highly regulated means that they meet federal regulations, not that they fully understand their role in better securing the organization as well as themselves. That, coupled with seeking higher levels of adoption for unwritten security rules, is likely to have a direct impact on the overall positive movement of these two critical areas.



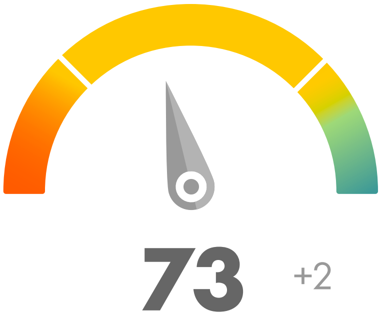
Employee knowledge, interactive security content, as well as pervasive and continuous communications are all critical drivers to reinforce the importance to how security-related behaviors are perceived by employees as normal and accepted or unusual and unacceptable.

# Legal

Legal is largely impacted by the COVID-19 pandemic. Many legal services switched to remote work and as a result, the established norms of transactional work as well as dispute resolution had to adapt to this new form of engagement. Cybersecurity and privacy lawyers appear to be in greater demand due to the increase in cyber attacks. Legal practices that facilitate the collection and protection of data have thrived.

A well-organized sector, many collaborations formed to quickly address the threat of bad actors regarding the large amounts of sensitive client data and financial transactions. The benefit from these collaborations is reflected in the overall increases in security culture that finds Legal at 73, up two points over last year.

All but one dimension saw improvement over last year's ratings. Legal firms are overwhelmingly positive towards Norms, which increased a substantial four points to 71 this year. Attitudes and Responsibilities both increased by two, now rating at 76 and 71.

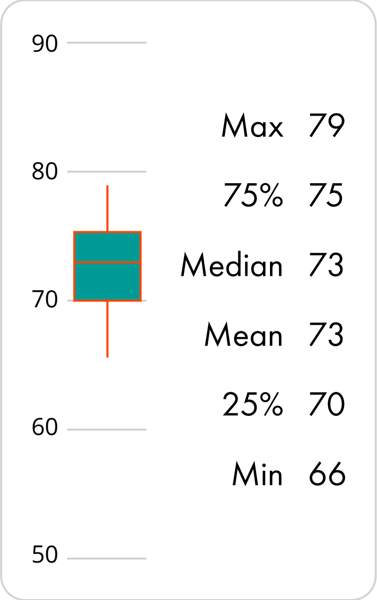


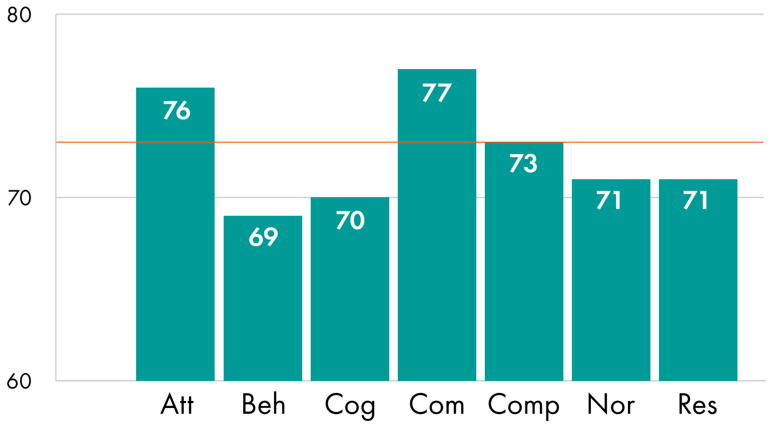
26

2,522

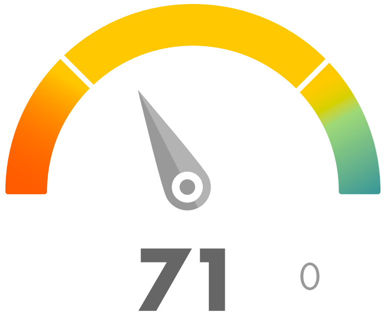
## Areas for Improvement

With the Behavior dimension scoring 69, a one-point decrease from last year, it is clear that more focus should be placed on conduct and adaptation to new remote environmental norms. And despite great improvement in both Norms (71) and Responsibilities (71) there is much room for improvement. As with last year's findings, it is important to note the correlation between Behaviors and Norms; an increased focus on reinforcing Norms to drive desired Behaviors, particularly in the current remote work environment, is recommended.





# Manufacturing

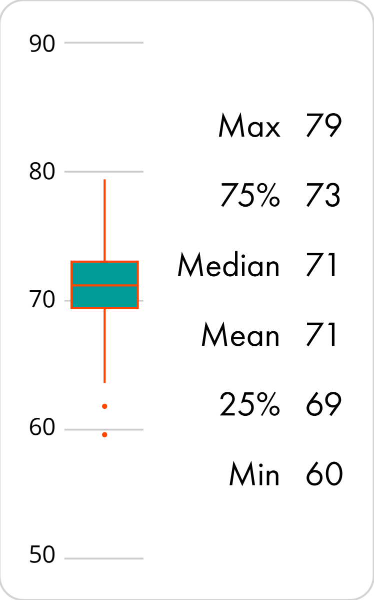


129

20,884

As with most sectors, COVID-19 has changed how manufacturers conduct their business. The pandemic created the greatest disruption to manufacturing since the second World War. Many employees began work from home and bad actors are targeting companies now more vulnerable due to the worldwide disruption of supply chain materials; this is causing the Manufacturing sector's journey towards digital transformation for supply chain, globalization and increased connectivity of manufacturing platforms to slow. These rapidly evolving factors contribute to the Manufacturing sector, again receiving a moderate security culture score of 71.

The Manufacturing sector experienced a slight increase in the Compliance dimension from 70 to 71, possibly due to renewed policy awareness as a result of global supply chain disruption. Unfortunately, this success is offset by the sector's steady ratings in three dimensions (Cognition (67), Communication (76), Norms (69)) and, significantly, the loss of one point in three other dimensions (Attitude (74), Behavior (71), Responsibility (70)).



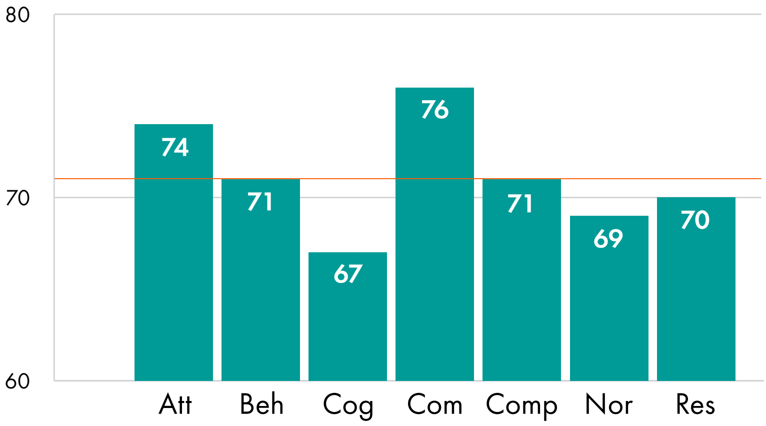
The Communication dimension remains consistent (76) and with one of the highest scores of this dimension in any industry, clearly demonstrating their information avenues are available and utilized by its employee base.

Both the Norms and Cognition dimensions remain in place. The Norms dimension measured at 69, indicates the unwritten rules and how they are being adopted by the employees and at 67, the Cognition dimension is a clear indicator that despite the consistent score, the Manufacturing sector has more work to do regarding risk and threat awareness.

## Areas for Improvement

The sector's slight dip in the Attitudes dimension from 75 to 74 indicates a slight decline in employees' willingness to adopt security practices in keeping with this sector's evolution as it confronts pandemic-related challenges.

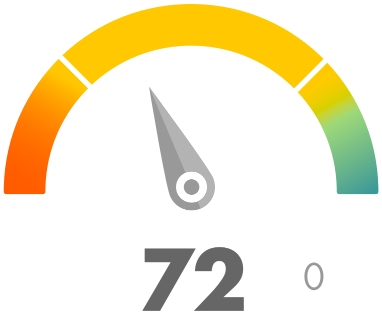
The Behaviors dimension looks at how employees behave regarding security, and this dimension has lost one point, now at 71. Similarly, the Responsibility dimension decreased one point last year, now at 70.



The Manufacturing sector is one of the most besieged and vulnerable to phishing attacks; as such, improvement in Attitudes, Behaviors and Responsibilities, in addition to bolstering other vulnerable areas via improved training and education programs will better defend against ongoing cyber threats.

# Not for Profit

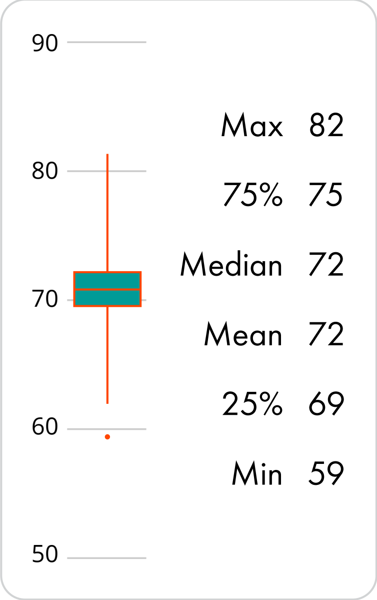
Cybercriminals continue to target Not for Profit organizations, knowing that they generally have very lean operating budgets and can sometimes justify only a small investment back into operations. As a result, cybersecurity is often neglected. In a time of unprecedented unemployment, the growing need for food banks and ongoing government-funded relief efforts, they are part of the critical infrastructure and as a result, ripe for a cyber attack. Many Not for Profits exist on the fringe of what is considered a small business and do not believe they are big, important or relevant enough to provide a big payday. But times are very different now, and their bounty has gone up. With an overall security culture score of 72, Not for Profits depend heavily on their favorable brands, strong reputations and word-of-mouth marketing to drive dollars, volunteers and interest toward their causes.



113

9,652

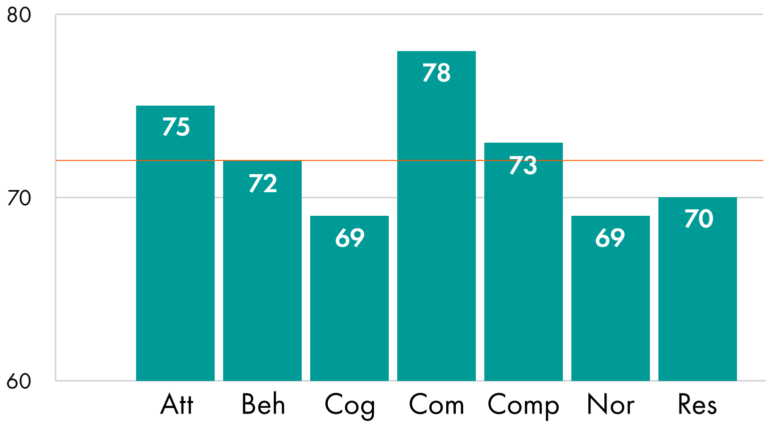
For the second year, Not for Profits scored best in the dimension of Communication (78—unchanged from 2020), showing strong attitudes toward the act of communicating. This makes sense, since communicating is where they invest a lot of time and money to draw interest. Since communicating is a critical component of building a strong security culture, it is important that Not for Profits cascade the right security information to the right audiences at the right time, both internal and external, raising donor long-term trust and confidence.



## Areas for Improvement

Most of the dimensions for Not for Profits fell in the moderate scoring range, with Cognition and Norms at 69, a one-point decrease in Norms at the lower half of this range. With less to invest that is deemed non-essential and while focused on the primary goal of pursuing the organization's objectives while keeping the doors open, Not for Profits tend not to rank security training as a top priority. Therefore, personnel and volunteers have varied levels of knowledge of security best practices.

A lack of overall security knowledge results in the low adoption rate of critical, unwritten security rules, which will impact overall secure behaviors and lead to operating under a less secure culture. Not for Profits would benefit in leveraging low cost or free security tools that are developed for their specific needs. That way, investment in the form of dollars is less of an obstacle, and they can focus their time and energy on enrollment, engagement and adoption of relevant messaging for their varied audiences.



# Other

**73** +1

164

17,788

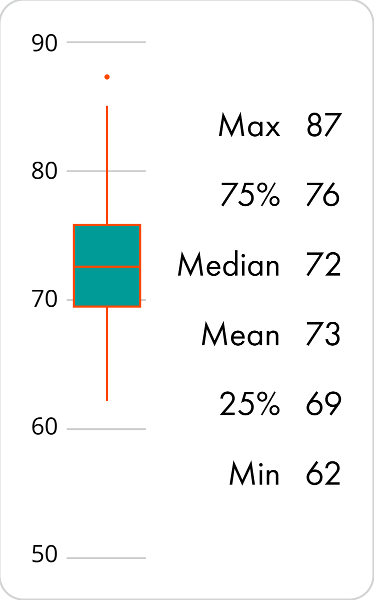
The Other sector, with an overall security culture score of 73, represents industries that did not fit into the named industry sectors, or in which the data available in a named sector was less than 10 organizations.

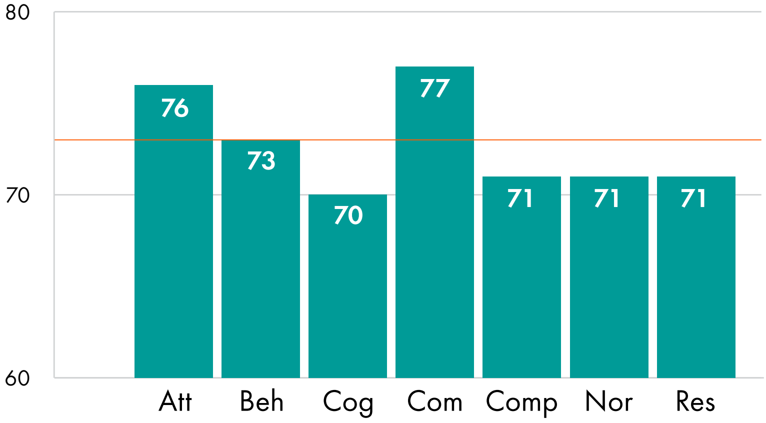
Across this grouping, Communication scored moderate with a 77, a one-point increase from last year. While Attitudes also scored in the moderate range with a score of 76, a one-point increase from last year. With moderate scores in both Communication and Attitudes, it is likely that employees are open to making necessary adjustments to adopt more secure practices. Additionally, their Communication score demonstrates that they are working to have effective channels for the creation and dissemination of messaging to their respective audiences across different areas.

## Areas for Improvement

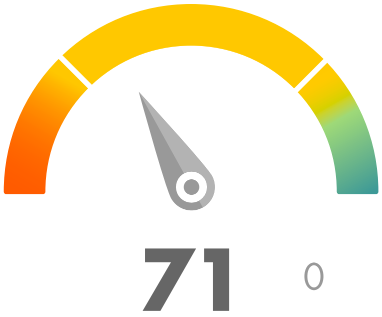
The Other sector is showing a moderate score of 70 in Cognition, a two-point increase from last year. The Cognition score shows that there is a strong need for more frequent, comprehensive and engaging security awareness training programs. With such diverse groups of industries, representing a diversity of employee backgrounds with equally diverse skill sets and degrees of security knowledge, the Other sector's ability to find and assign appropriately targeted, relevant security content to meet the needs of their diverse audience is critical for success. Additionally, access to multiple mediums for training delivery will help to bring training content to the individuals so that they can consume it when they have time instead of forcing them into a more traditional training cycle.

In the dimension of Norms, the Other sector should be evaluating how their employees are influenced and guided by their organization's unwritten rules. As a key overall influencer, Norms can be leveraged to drive more awareness to security behaviors across the employee base to strengthen the security culture.





# Retail and Wholesale

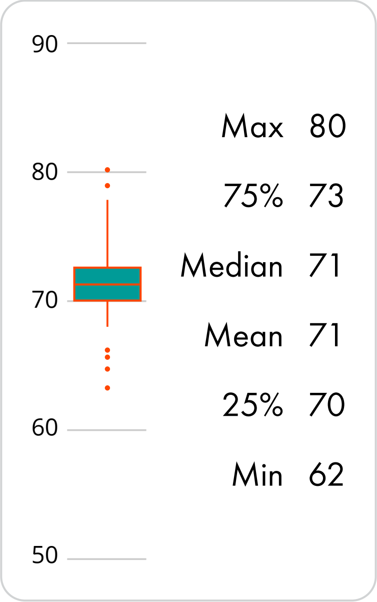


79

20,628

The Retail and Wholesale sector has traditionally been a favored target among cybercriminals. The challenge is, as always, finding a balance between fulfilling the needs of customers while increasing their overall security posture. In a time where consumers are looking for greater convenience and safety in their shopping options, online sales are growing while traditional storefronts are struggling. Also, if entities were struggling pre-COVID-19, the likelihood of them faltering increases because with higher levels of unemployment, spending that may have gone towards "extras", is now straining to put food on the table in many households. Consumers are also looking at discount options to fulfill what they need. Instead of shopping at well-established and trusted retailers, they will often select the discount retailer to maximize their spend.

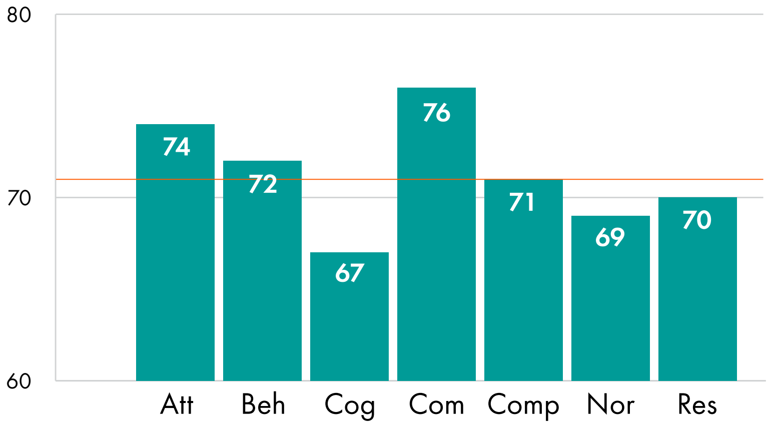
The Retail and Wholesale sector, with an overall security culture score of 71 indicates a moderately low attitude toward security. With a moderate score of 74 in the Attitudes dimension, a one-point decrease from last year, it is likely that employees in this sector are positive toward making adjustments and adopting security best practices. Further, communication is the strongest aspect of Retail and Wholesale security culture, with a Communication dimension at 76, unchanged from 2020. This industry is finding ways to disseminate relevant security-related content across their diverse audience in a way that is meaningful and useful. The approach here is not one size fits all, but rather looking at each job function and determining what would be most helpful and actionable for those roles.

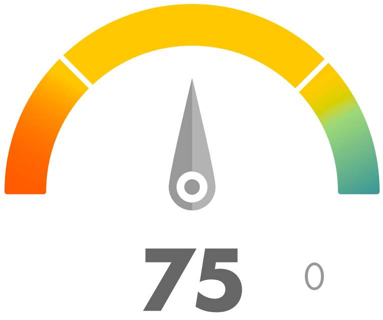


## Areas for Improvement

The Retail and Wholesale sector has opportunities for improvement on the Norms dimension with a score of 69, unchanged from 2020. This dimension is measuring the unwritten rules and how employees are adopting them. Although job-related training may be more individualized by role, every employee needs to understand and adopt those common sense, unwritten security-related rules.

The Cognition dimension is another area where the Retail and Wholesale sector can improve. With a score of 67, unchanged from 2020, the lowest rated dimension in this sector, there is a clear need for improved training and education programs. There is a strong connection between Cognition and Norms, and the Retail and Wholesale sector is likely to see direct improvement in overall security culture by emphasizing training in both dimensions.





195

59,529

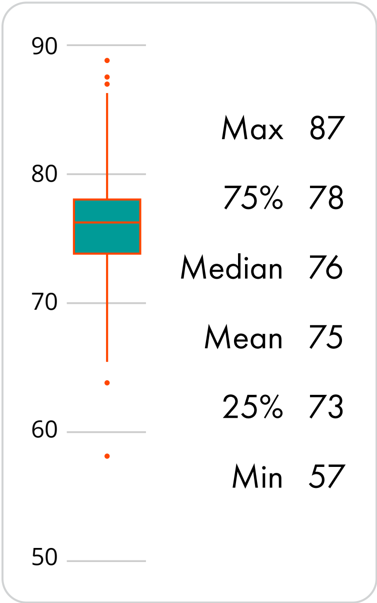
## Technology

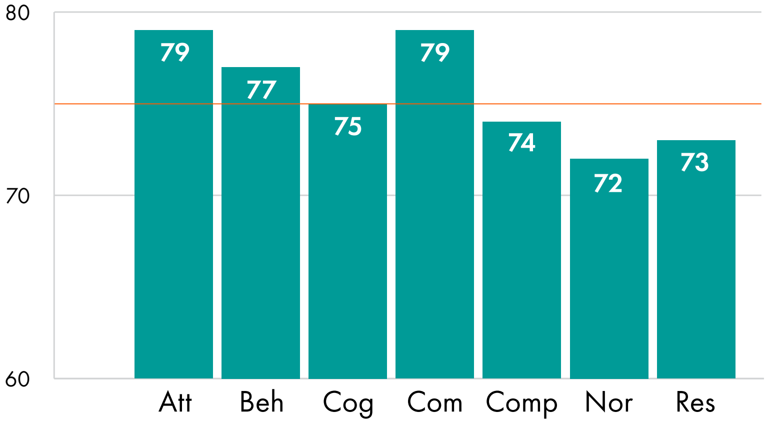
Technology companies have dramatically shifted priorities to support pandemic-related needs: business continuity, remote work and planning for transition to the "new normal", which will likely include a large portion of their workforce maintaining a work from home status. This pivot included bolstering their remote workforce's network security as well as training end users to identify new threats that bad actors pose by targeting the remote workforce. These adjustments are reflected in the Technology sector's moderate security culture score of 75.

Perhaps as a result of these shifts in priorities, the Technology sector has increased in five out of seven dimensions, most notably in Behaviors and Cognition, which both increased two points to 77 and 75, respectively. The highest dimension, as with last year, was in the Attitudes dimension, which increased one point to 79 this year. It is again clear that employees in this industry exhibit an understandable inclination towards making adjustments and adopting security practices.

### Areas for Improvement

The Technology sector's areas for improvement are minor with decreases in two dimensions, Norms (72) and Responsibilities (73). As mentioned previously in this assessment, the dramatic shift in the industry due to the pandemic is reflected in these scores, due to a rapid adjustment in what is the "new normal" and what employees' new work from home responsibilities are in a work from home environment.





# Transportation

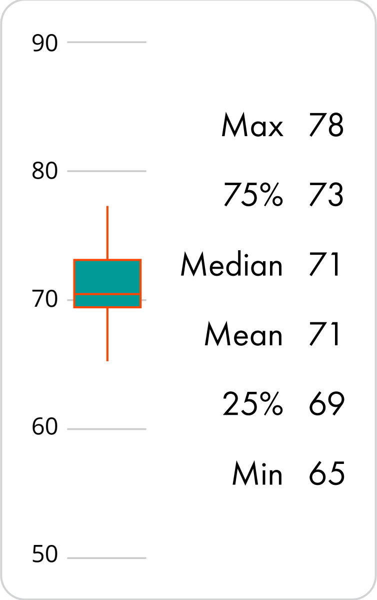
The pandemic has amplified existing security culture likely due to increased dependencies upon Transportation as the population has increasingly leveraged online shopping and home delivery services. The potential long-term result of a sustained move from storefront to online shopping will continue to drive the industry's security evolution. Additionally, the global population was at a standstill. There were reductions in all forms of transportation, from air travel to road travel. This transformation is evident given the industry's overall security culture improvements, to include an overall score that has increased one point over last year, but is still moderately low at 71.

Transportation improved in five out of seven dimensions, most notably in the Compliance dimension, which improved two points over last year's assessment. In addition, Attitudes, Behavior, Norms and Responsibilities are all up one point. With the industry increasingly dependent upon digital infrastructure, their security culture—particularly as it relates to cyber hygiene—is increasingly vital. This increased digital dependency increases their cyber attack surface, making users more at risk to social engineering.

71 +1

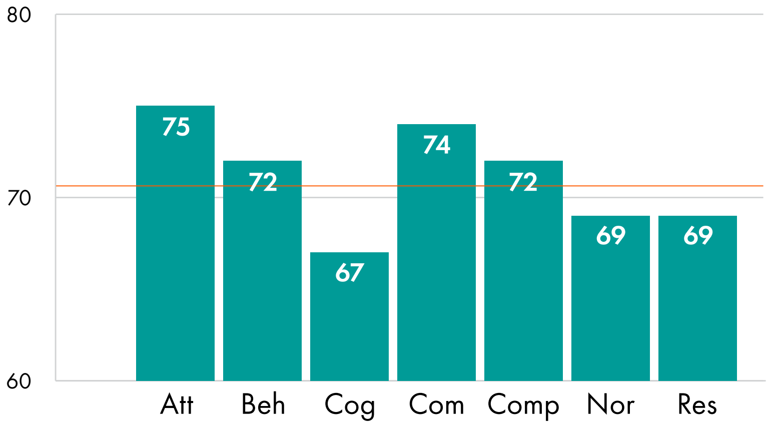
23

8,501



## Areas for Improvement

Specific opportunities for improvement can focus on both Cognition (which did not change from last year at 67) and Communications, which fell one point to 74. However, as with last year's assessment, the Transportation sector can also benefit from a holistic approach on all dimensions to elevate this sector's overall security culture.



*Of 1,161 security leaders surveyed in 2020,* ***94%*** *reported that* ***security culture is the most important element*** *in their security strategy.*

# Methodology and Data

This report was created by KnowBe4 Research. The report leverages anonymized data from KnowBe4's Security Culture Survey. The sample size represents 2,093 surveyed organizations around the world, with more than 328,173 employees across 17 industry sectors, effectively making this the largest report of its kind published to date.

Below is a description of the methods used to analyze the data along with descriptive tables.

## How Data Was Collected

The data for this report was collected using the Security Culture Survey, which is available to KnowBe4 customers via the Kevin Mitnick Security Awareness Training (KMSAT) platform. The Security Culture Survey was developed by CLTRe, a KnowBe4 company, based on a scientific approach that integrates survey methodology, statistics and scientific findings from security culture research and psychometrics. The survey consists of four items for each distinct dimension of security culture, a total of 28 items; and the question set and methodology have been refined over several years. The data collection period was from November 2019 through December 2020 and represents customers around the globe. The data for this report is based on a single data collection time point for each employee and was then anonymized and aggregated. All data analysis was performed in the software environment R (r-project.org).

## Data Preprocessing

To ensure validity and reliability, the data was cleaned before any calculations were conducted. Industry sectors with less than 10 organizations, or where industry sector information was not available, were moved to the Other industry category. The industries that were moved to Other included Hospitality and Internet and Software Services. A listwise deletion of missing data was conducted, which means that responses with missing values were deleted.

Furthermore, respondents who spent less than two minutes on the survey were excluded, as they would not have taken the time to read the questions before answering them. Organizations with less than 10 valid employee responses were excluded, as these were considered accounts for testing the survey and thus do not measure a representative proportion of the organization.

## Statistical Analyses

The values that employees provide on the 28 security culture items are transformed into eight metrics for each organization. The first seven metrics correspond to each of the seven security culture dimensions. The final metric is the Security Culture Score, which is calculated by taking the mean of all the dimension scores. All scores have a range from zero to 100.

The Security Culture Survey, and therefore this report, is created as a multi-level statistical analytics tool, where individual respondents are aggregated to the level of an organization. One of the benefits of aggregating scores to an organization level rather than at the employee level, is that the effects of organization size on industry benchmarks were neutralized. The unique algorithm for this transformation was designed by CLTRe and based on a complex conceptual understanding of organizational security culture.

After statistical analysis, the scores were compared to the Security Culture Index. The Security Culture Index is the scale used to measure security culture, and consists of these five levels.

| Poor | Mediocre | Moderate | Good | Excellent |
|---|---|---|---|---|
| 0 up to 60 | 60 up to 70 | 70 up to 80 | 80 up to 90 | 90 up to 100 |

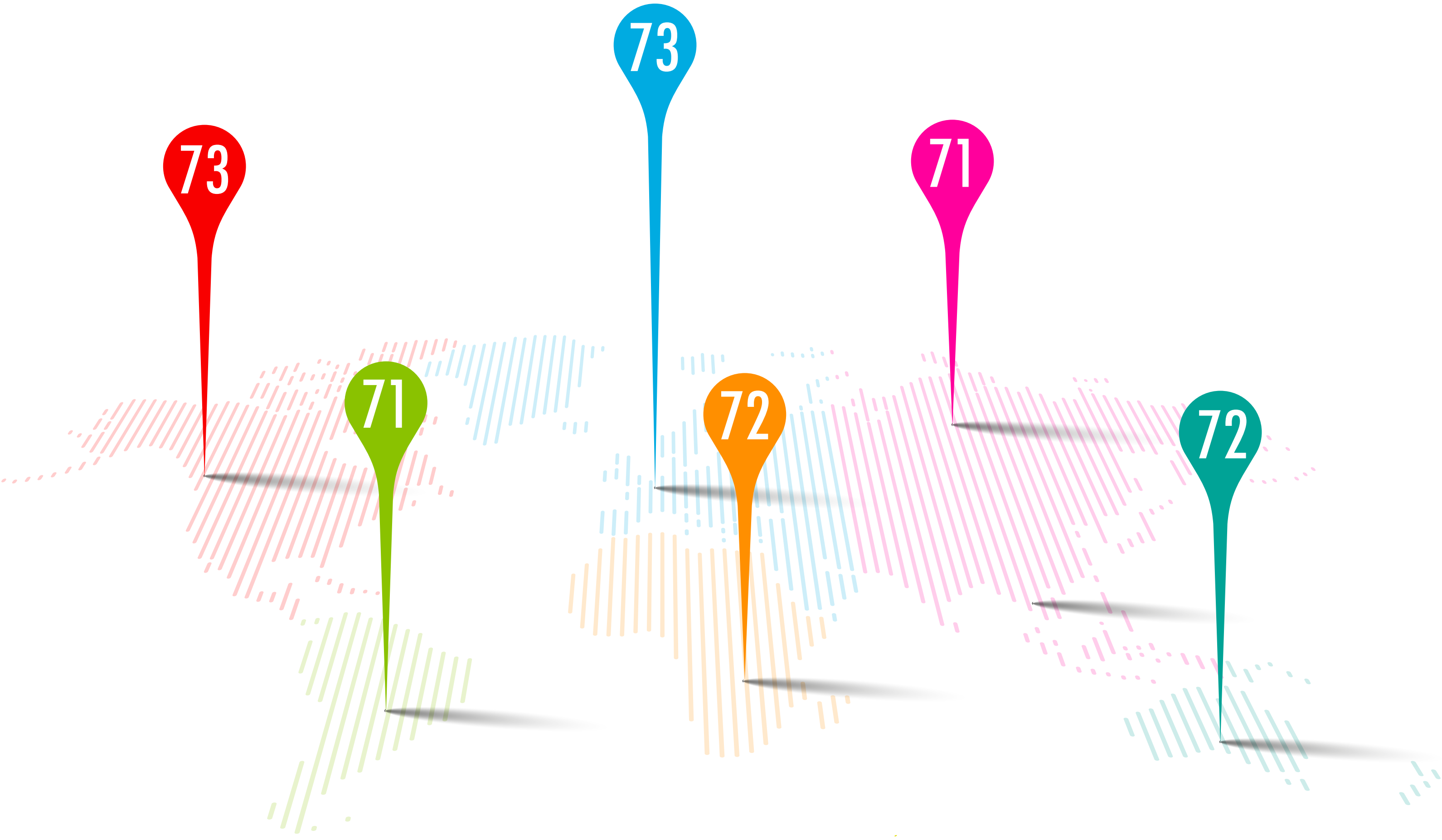
## Data Size

The data consists of 328,173 employees and 2,093 organizations. After data cleaning, the final sample consists of 321,609 employees and 1,872 organizations that completed the Security Culture Survey. Data was collected from 49 countries.

*Table: Frequencies of employees and organizations with complete data per industry*

| Industries | Organizations | Employees |
|---|---|---|
| Banking | 148 | 36,710 |
| Business Services | 130 | 12,867 |
| Construction | 48 | 6,815 |
| Consulting | 69 | 5,975 |
| Consumer Services | 35 | 4,986 |
| Education | 62 | 8,590 |
| Energy & Utilities | 69 | 10,129 |
| Financial Services | 261 | 32,299 |
| Government | 133 | 30,951 |
| Healthcare & Pharmaceuticals | 123 | 17,725 |
| Insurance | 65 | 15,058 |
| Legal | 26 | 2,522 |
| Manufacturing | 129 | 20,884 |
| Not for Profit | 113 | 9,652 |
| Other | 164 | 17,788 |
| Retail & Wholesale | 79 | 20,628 |
| Technology | 195 | 59,529 |
| Transportation | 23 | 8,501 |
| **Total** | **1872** | **321,609** |

# Regional Data



In this report, data from the following regions and countries has been examined. The table Region is an aggregation of the data up to geographical regions. The map shows the scores across the world.

In the table below, the security culture scores, number of organizations and number of employees are shown as our dataset contains per country.

*Table: Region*

| Region | Score | Organizations | Employees |
|---|---|---|---|
| Africa | 72 | 39 | 32,442 |
| Asia | 71 | 15 | 7,301 |
| Europe | 73 | 100 | 22,828 |
| Latin America | 71 | 8 | 1,075 |
| North America | 73 | 1612 | 246,348 |
| Oceania | 72 | 47 | 6,730 |
| Other[1] | 72 | 51 | 4885 |

[1] The category Other is for where region data is not available.

| Country | Score | Employees | Organizations |
|---|---|---|---|
| NA | 72 | 4,885 | 51 |
| Australia | 71 | 5,609 | 37 |
| Bahamas | 71 | 30 | 1 |
| Belgium | 70 | 976 | 3 |
| Belize | 71 | 193 | 1 |
| Bermuda | 73 | 408 | 2 |
| Botswana | 71 | 84 | 1 |
| Canada | 72 | 10,023 | 100 |
| Cyprus | 82 | 16 | 1 |
| Denmark | 74 | 85 | 1 |
| Eswatini | 74 | 15 | 1 |
| Finland | 69 | 147 | 2 |
| France | 67 | 1,241 | 3 |
| Ghana | 67 | 34 | 1 |
| Gibraltar | 81 | 10 | 1 |
| Greece | 72 | 2,165 | 2 |
| Guatemala | 73 | 19 | 1 |
| Hong Kong | 69 | 1,241 | 1 |
| India | 78 | 2,588 | 3 |
| Ireland | 70 | 346 | 3 |
| Kenya | 74 | 601 | 3 |
| Luxembourg | 78 | 143 | 2 |
| Malaysia | 62 | 1,396 | 1 |
| Malta | 70 | 83 | 3 |
| Mauritius | 68 | 371 | 1 |
| Mexico | 77 | 539 | 3 |
| Mozambique | 66 | 114 | 1 |
| Namibia | 77 | 32 | 1 |
| Netherlands | 76 | 371 | 4 |
| New Zealand | 73 | 1,121 | 10 |
| Nigeria | 71 | 125 | 2 |
| Norway | 69 | 227 | 1 |
| Oman | 71 | 121 | 2 |
| Philippines | 76 | 181 | 4 |
| Rwanda | 71 | 15 | 1 |
| Saint Lucia | 77 | 15 | 1 |
| Saudi Arabia | 72 | 65 | 1 |
| Singapore | 69 | 1,895 | 6 |
| Sint Maarten (Dutch part) | 66 | 47 | 1 |
| South Africa | 74 | 29,693 | 23 |
| Suriname | 66 | 262 | 1 |
| Sweden | 73 | 80 | 1 |
| Switzerland | 70 | 1,352 | 2 |
| Tanzania, the United Republic of | 77 | 482 | 1 |
| United Arab Emirates | 76 | 125 | 3 |
| United Kingdom | 74 | 15,275 | 66 |
| United States | 74 | 235,887 | 1509 |
| Zambia | 74 | 785 | 1 |
| Zimbabwe | 76 | 91 | 2 |

# Authors

## Anita-Catrin Eriksen

Anita-Catrin Eriksen is a researcher with a social science background who enjoys applying her knowledge and skills to new areas. She loves working with data in programming languages, like R and Python, to produce accessible knowledge and insight. As the security culture researcher at CLTRe, a KnowBe4 company, she manages, analyses and interprets data. Eriksen also oversees research projects and produces papers. She holds a Bachelor of Arts from University College Utrecht in the Netherlands, and a Master of Science in Social Psychology from the University of Edinburgh in the UK. Her academic work mainly focused on attitudes, social identities, culture, statistics and survey methodology.

## Kai Roer

Kai Roer (author of "Build a Security Culture" by publisher IT-Governance) has over 25 years of experience in cybersecurity, with much of his expertise centered around security culture. He is currently managing director of CLTRe, a KnowBe4 company, and managing director of KnowBe4 Research, where he is responsible for security culture research. Prior to founding CLTRe, Roer created the global de-facto standard Security Culture Framework. His groundbreaking research into security culture metrics provides organizations worldwide with deep insights into the human factors that influence risk and security. Roer is an award-winning specialist on security behaviors and security culture as well as a best-selling author. He is the host of the videocast Security Culture TV and an avid blogger. Roer keynotes at events around the world. He belongs to the Norway Chapter of the Cloud Security Alliance.

## Dr. Gregor Petrič

Dr. Gregor Petrič is an accomplished researcher and academic in the social scientific space, with a specialization in socio-informatics. He oversees that the research projects are of the required standard and quality. Petrič co-created the CLTRe security culture survey tool and analytics with Kai Roer. He is internationally well known for his advances in measurement of social science phenomena and applying structural models to explanation of internet-related social and cultural phenomena. He is also an expert in web survey methodology. He published numerous papers in top-end journals in the fields of information society, methodology of social science research and e-health. He serves as the head of the Centre for Methodology of Informatics (Faculty of Social Sciences, University of Ljubljana), where he was awarded full professor in 2019.

## Joanna Huisman

Joanna Huisman is senior vice president of strategic insights and research at KnowBe4. She is a marketing, training and communications professional with over 20 years of experience in strategic, internal and customer-facing engagements in the financial services/tech industries with added experience in sales, operations and organizational development. Huisman was previously senior research director at Gartner in the areas of security awareness, education, behavior management, culture, crisis communications, security and risk program management. Prior to that, she was senior director of global security communications, training, and awareness for ADP. Huisman earned a B.A. in Government and Politics from Widener University.

## Rosa L. Smothers

Rosa L. Smothers has over 20 years of experience in cybersecurity. She is currently senior vice president of cyber operations at KnowBe4, where she is responsible for leading KnowBe4's Federal Practice efforts, including providing cybersecurity advisory services to civilian and military agencies within the U.S. federal government. Ms. Smothers is also responsible for providing analysis for KnowBe4's cybersecurity research and cyber threat intelligence efforts. Having served for over a decade in the Central Intelligence Agency, Ms. Smothers is a highly decorated national security professional with extensive experience leading the planning and execution of cyber operations against terrorist and nation-state targets, as well as the adoption of cutting-edge computer technology. She served as a cybersecurity analyst and technical intelligence officer in the Center for Cyber Intelligence and the Counter Terrorism Mission Center and on multiple overseas tours, including extensive service in Iraq. She holds a B.A. in Information Studies from Florida State University and an M.S. in Computer Network Security from Capitol Technology University. Ms. Smothers is a mentor to women and young people in cybersecurity and is a member of Infragard.

## Perry Carpenter

Perry Carpenter (author of, "Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors" from Wiley Publishing) currently serves as chief evangelist and strategy officer for KnowBe4. In previous roles, Perry led security awareness, security culture management and anti-phishing behavior management research at Gartner Research, in addition to covering areas of IAM strategy, CISO Program Management mentoring and Technology Service Provider success strategies. With a long career as a security professional and researcher, Mr. Carpenter has broad experience in North America and Europe, providing security consulting and advisory services for many of the best-known global brands. Perry holds a Master of Science in Information Assurance (MSIA) from Norwich University in Vermont and is a Certified Chief Information Security Officer (C|CISO).

## CLTRe, a Research Division of KnowBe4

CLTRe AS was established by Dr. Gregor Petrič and Kai Roer in 2015 in order to answer the information security industry's need for a way to measure and understand the impact of security culture. The groundbreaking work is a prime example of applying science in the real world. CLTRe AS was acquired in 2019 and is now known as KnowBe4 Research AS. It is committed to bringing its research to the world in order to help understand the human factors that influence security.

### KnowBe4 Research

KnowBe4 Research is a special projects division of KnowBe4, Inc. Our mission is to provide IT and security leaders with high quality, vendor neutral data-driven insights related to cybersecurity and the human element.

### KnowBe4, Inc.

KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, is used by more than 35,000 organizations around the globe. Founded by IT and data security specialist Stu Sjouwerman, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud and other social engineering tactics through a new-school approach to awareness training on security. Kevin Mitnick, an internationally recognized cybersecurity specialist and KnowBe4's Chief Hacking Officer, helped design the KnowBe4 training based on his well-documented social engineering tactics. Tens of thousands of organizations rely on KnowBe4 to mobilize their end users as the last line of defense.

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com

V031821