



# Measure to Improve

Security Culture Report 2020

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

## Table of Contents

<b>Introduction</b>	4
Summary of Findings	5
The Security Culture Disconnect	7
<b>Industry Comparison</b>	9
How to Read the Chart	10
Comparing Security Culture Scores Across Industries	11
Figure: Comparing Security Culture Scores	12
Table: Comparing Security Culture Scores	12
Comparing Attitudes	13
Figure: Comparing Attitude Scores	14
Table: Comparing Attitude Scores	14
Comparing Behaviors	15
Figure: Comparing Behavior Scores	16
Table: Comparing Behavior Scores	16
Comparing Cognition	17
Figure: Comparing Cognition Scores	18
Table: Comparing Cognition Scores	18
Comparing Communication	19
Figure: Comparing Communication Scores	20
Table: Comparing Communication Scores	20
Comparing Compliance	21
Figure: Comparing Compliance Scores	22
Table: Comparing Compliance Scores	22
Comparing Norms	23
Figure: Comparing Norm Scores	24
Table: Comparing Norm Scores	24
Comparing Responsibilities	25
Figure: Comparing Responsibilities Scores	26
Table: Comparing Responsibilities Scores	26
<b>Industry Benchmark</b>	27
How to Read the Industry Page	27
How to Read the Box Plot	27
How to Read the Column Chart	27
The Security Culture Index	27
Banking	28
Areas for Improvement	28
Statistics for Banking	29
Business Services	30
Areas for Improvement	30
Statistics for Business Services	31
Construction	32
Areas for Improvement	32
Statistics for Construction	33
Consulting	34
Areas for Improvement	34
Statistics for Consulting	35
Consumer Services	36
Areas for Improvement	36
Statistics for Consumer Services	37

<b>Education</b> .....	38
<i>Areas for Improvement</i> .....	38
<i>Statistics for Education</i> .....	39
<b>Energy &amp; Utilities</b> .....	40
<i>Areas for Improvement</i> .....	40
<i>Statistics for Energy &amp; Utilities</i> .....	41
<b>Financial Services</b> .....	42
<i>Areas for Improvement</i> .....	42
<i>Statistics for Financial Services</i> .....	43
<b>Government</b> .....	44
<i>Areas for Improvement</i> .....	44
<i>Statistics for Government</i> .....	45
<b>Healthcare &amp; Pharmaceuticals</b> .....	46
<i>Areas for Improvement</i> .....	46
<i>Statistics for Healthcare &amp; Pharmaceuticals</i> .....	47
<b>Insurance</b> .....	48
<i>Areas for Improvement</i> .....	48
<i>Statistics for Insurance</i> .....	49
<b>Legal</b> .....	50
<i>Areas for Improvement</i> .....	50
<i>Statistics for Legal</i> .....	51
<b>Manufacturing</b> .....	52
<i>Areas for Improvement</i> .....	52
<i>Statistics for Manufacturing</i> .....	53
<b>Not for Profit</b> .....	54
<i>Areas for Improvement</i> .....	54
<i>Statistics for Not for Profit</i> .....	55
<b>Other</b> .....	56
<i>Areas for Improvement</i> .....	56
<i>Statistics for Other</i> .....	57
<b>Retail &amp; Wholesale</b> .....	58
<i>Areas for Improvement</i> .....	58
<i>Statistics for Retail &amp; Wholesale</i> .....	59
<b>Technology</b> .....	60
<i>Areas for Improvement</i> .....	60
<i>Statistics for Technology</i> .....	61
<b>Transportation</b> .....	62
<i>Areas for Improvement</i> .....	62
<i>Statistics for Transportation</i> .....	63
<b>Regional Data</b> .....	64
<b>About the Report</b> .....	66
<b>Methodology</b> .....	66
<i>How Data was Collected</i> .....	66
<i>Data Preprocessing</i> .....	66
<i>Statistical Analyses</i> .....	66
<i>Data Size</i> .....	66
<b>Authors</b> .....	69
<b>CLTRe, a Research Division of KnowBe4</b> .....	72
<b>KnowBe4 Research</b> .....	72
<b>KnowBe4, Inc.</b> .....	72

# Introduction

2020 is a good year for the Security Culture Report. Since first introducing this report in 2017, we've been on a quest to provide security professionals and organizations with the most comprehensive study of cybersecurity culture-related data possible, comparing cybersecurity culture across as many industries and countries as possible.

In 2019, CLTRe was acquired by KnowBe4<sup>[1]</sup>, the provider of the world's largest security awareness training and simulated phishing platform, currently serving over 34,000 client organizations globally. After the acquisition, we spent several months integrating CLTRe's secret sauce, the Security Culture Survey, into KnowBe4's platform and were able to launch at the end of 2019<sup>[2]</sup>. Then we waited for the lifeblood of all studies: data.

In the 2020 report, we collected data from 120,050 employees in 1,107 organizations across 24 countries. The data was then anonymized and aggregated. We analyzed 17 industry sectors in detail. They are:

- Banking
- Financial Services
- Insurance
- Consulting
- Business Services
- Technology
- Healthcare & Pharmaceuticals
- Consumer Services
- Not for Profit
- Other
- Retail & Wholesale
- Legal
- Manufacturing
- Government
- Construction
- Energy & Utilities
- Transportation



---

1 KnowBe4 Acquires CLTRe: Shines Spotlight on Security Culture Measurement  
<https://www.knowbe4.com/press/knowbe4-acquires-cltre-shines-spotlight-on-security-culture-measurement>

2 KnowBe4 Assessments Help Gauge Proficiency of Your Users Security Awareness and Sentiment Towards Security Culture  
<https://blog.knowbe4.com/new-feature-knowbe4-assessments-help-gauge-proficiency-of-your-users-in-security-awareness-and-sentiment-towards-security-culture>

# Summary of Findings

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 cybersecurity culture-related strengths and weaknesses of individuals, organizations, industry sectors, regions and more. We systematically evaluate culture across seven distinct dimensions; they are:

Dimension	Definition
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

We calculated the strength of each dimension based on a proprietary statistical algorithm that provides an indexed score from 0 to 100. We then categorize scores based on where they rank as follows:

- 90-100** Excellent
- 80-89** Good
- 60-79** Moderate
- 50-59** Poor to moderate
- 30-49** Poor
- 0-29** Extremely poor

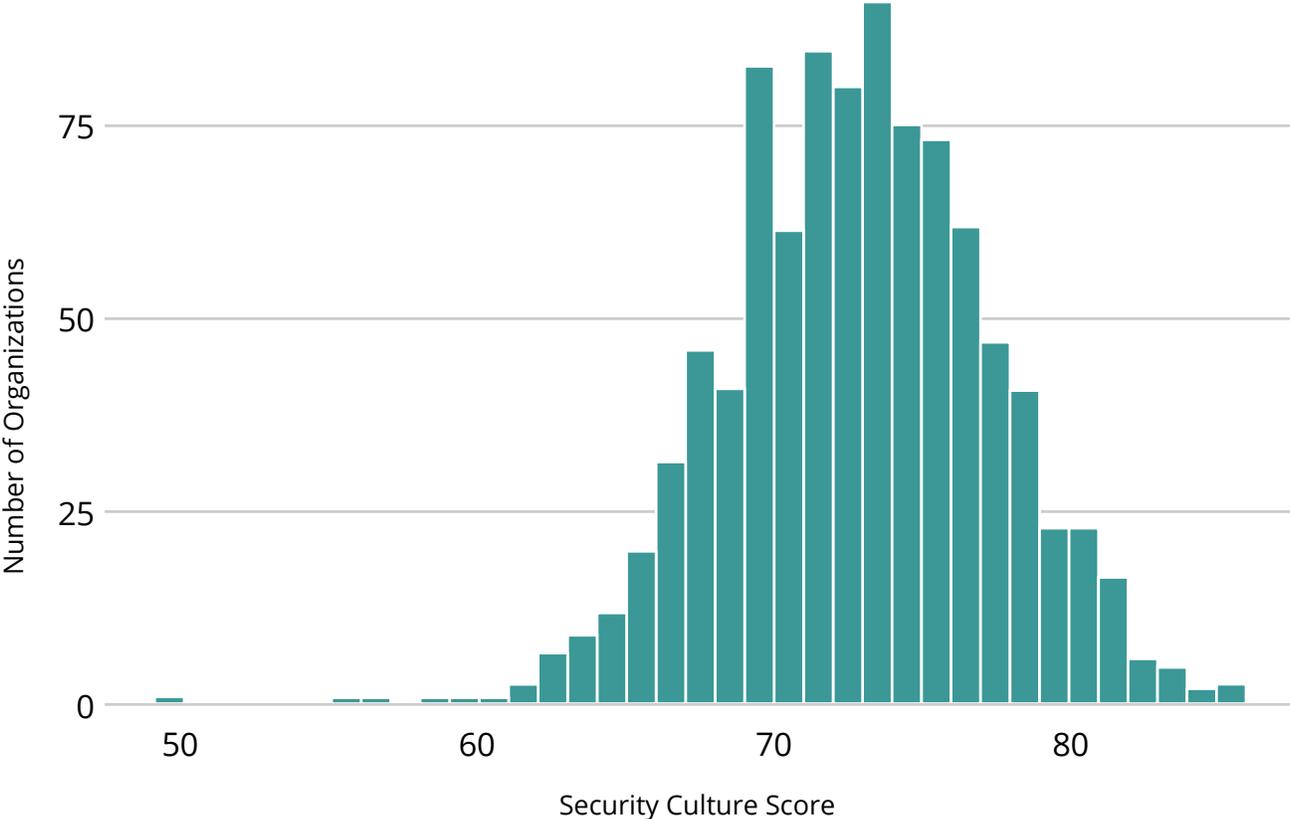
Results from this year's report revealed a large gap between the best performers and the poor performers. Unsurprisingly, the best performers were from Banking, Financial Services, and Insurance—all industries with a long tradition of managing risk. However, being a "best performer" doesn't necessarily equate to having performed at a desirable level, and they shouldn't be too quick to congratulate themselves. For instance, a score of 76, as seen by Banking and by Financial Services, is well below the expected level of 90 or above.

At the other end of the spectrum, we find Education, Transportation and Energy & Utilities. In our digital world, students and teachers are more reliant than ever on technology, and they need a solid grounding in security to protect themselves and their online systems.

With this in mind, the Education sector's poor security culture scores serve as a wake-up call. It is also important to note the poor security culture score exhibited by the Energy & Utilities sector. This is extremely concerning due to Energy & Utilities being part of critical infrastructure.

The figure below shows the distribution of all the organizations' security culture scores. The overall height of each bar represents the number of organizations with that security culture score. The analysis of maturity of security culture demonstrates variability among the 1,107 organizations analyzed, as the security culture score spans from a minimum of 50 to a maximum of 86.

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 (92%) of all analyzed organizations managed to develop a moderate security culture, while only a small portion (7%) of organizations have a good security culture. Alarming, a few organizations are scoring in the poor to moderate bracket and no organizations have reached an excellent security culture score yet.



# The Security Culture Disconnect

In 2020, Forrester Consulting conducted a study commissioned by KnowBe4<sup>[3]</sup>. The study looked at organizations' understanding and implementation of security culture, and it was conducted worldwide. The respondents were security professionals. This study demonstrated a disconnect between the perceived importance of security culture and the understanding of what security culture is.

Key findings from the Forrester study include:

- Although 94% of organizations agree security culture is important, security leaders have not agreed on what the term means.
- Decision makers gave us 758 unique definitions for security culture that fit into the following five unique categories:
  - Compliance with security policies (29%)
  - Awareness & understanding of security issues (24%)
  - A shared responsibility across the organization (22%)
  - Advocacy and support (14%)
  - Security embedded in the organization (12%)

Due to the increase in security breaches, it is common to think organizations are just trying to create a risk reduction mechanism when thinking about security culture. However, the study showed 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.

The study concludes that the inability to define such a huge initiative (security culture) leads to an over-confidence for organizations' security cultures. This lack of a common definition and understanding of the phenomena of security culture introduces a number of challenges for organizations' abilities to build and maintain security cultures.

Security culture needs to be defined in a way that makes it easy to understand, easy to measure and easy to manage. By defining security culture as *the ideas, customs and social behaviors of an organization that influence their security*<sup>[4]</sup>, it becomes clear that security culture is closely linked to culture. To work with 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<sup>[5]</sup> identifies phishing as the most common threat action. Research by KnowBe4<sup>[6]</sup> 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, KnowBe4 research shows the immediate role of security culture in lowering employee-induced risks in organizations<sup>[7]</sup>.

It is crucial to adopt a common definition of security culture. Only with a common understanding will we be able to have informed discussions on how to improve and transform security cultures to the levels required. By creating this universal understanding, organizations around the world will be able to learn from each other, benchmark against each other, and build a strong human firewall backed by technology and policies.

3 The Rise of Security Culture, a commissioned study conducted by Forrester Consulting on behalf of KnowBe4, April 2020

4 As defined by The Security Culture Framework, 2012

5 <https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf>

6 Phishing by Industry Benchmarking Report 2020 (<https://www.knowbe4.com/hubfs/2020PhishingByIndustryBenchmarkingReport.pdf>)

7 Risk Score vs Security Culture Score, CLTRe/KnowBe4 2020

A photograph of four business professionals walking in a modern office space. From left to right: a man in a light blue button-down shirt and khaki pants, a woman in a light pink top and dark pants, a woman in a white shirt and dark vest, and a man in a white button-down shirt and dark pants. They are all smiling and looking towards the right. The background shows office furniture, a staircase, and large windows with dark curtains. The image has a teal overlay.

*It is crucial to adopt a common definition of security culture.*

*Only with a common understanding will we be able to have informed discussions on how to improve and transform security cultures to the levels required.*



# Industry Comparison

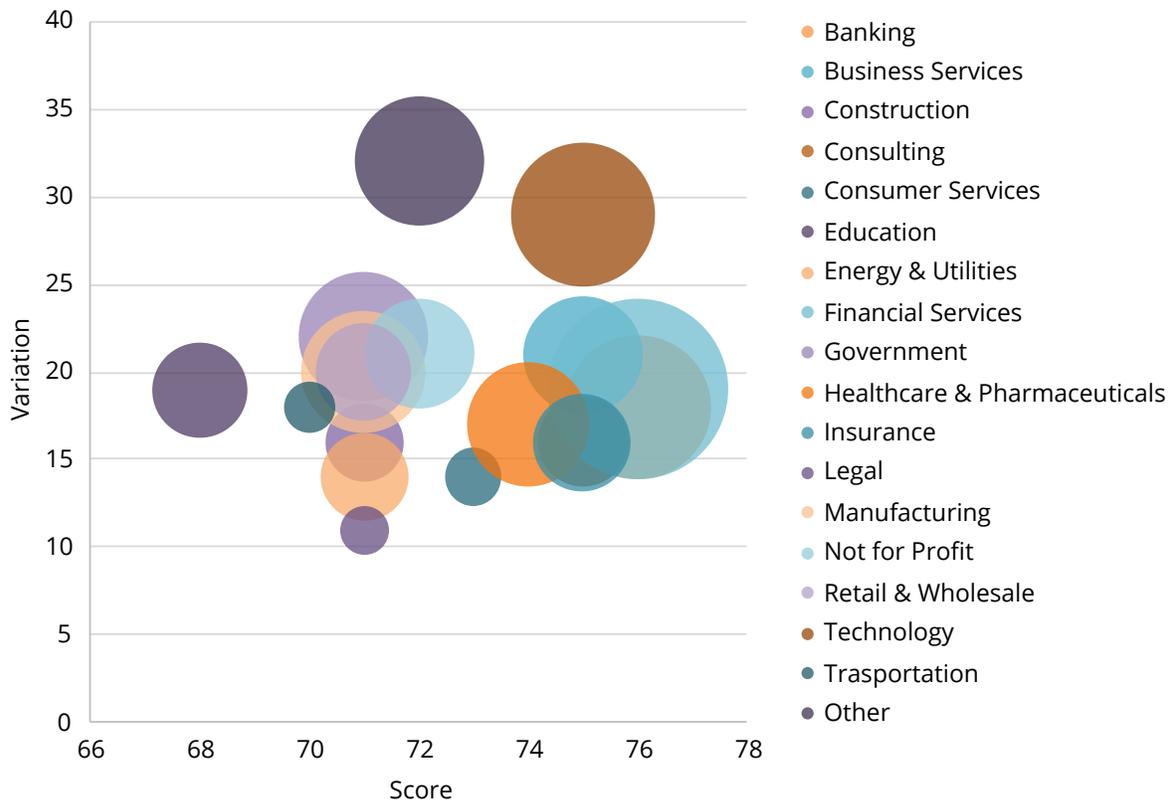
Security culture varies across industries. In the industry comparison section, we compare all industries according to their security culture scores. We also compare the industries across each of the seven dimensions of security culture.

Evaluating security culture through a standardized measurement instrument provides deep insights into how organizations are working with security culture and its influence on their risk. The KnowBe4 Security Culture Survey is a scientific measurement instrument designed specifically to provide an objective evaluation of an organization’s security culture across seven dimensions:

Dimension	Definition
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

In this report, we collected data from more than 120,000 employees from around the world. The data within the report shows that organizations in some industries are closer in their security culture scores. When organizations within an industry score closer together, we consider the industry’s security culture to be stronger. This can be seen in the chart on the following page, where each industry is represented with a bubble.

Variation vs. SCC vs. Sample Size



## How to Read the Chart

The size of the bubble measures the number of organizations within the industry. The value on the x-axis is the security culture score of that industry. The value on the y-axis is the strength of the culture. We define the strength of the culture to be the difference between the best and the worst performer within that industry sector—a smaller difference is a stronger culture, which requires more effort to change. A high security culture score, that is also showing a small difference between the best and the worst score, is a good thing: it will be more difficult to change such a culture for the worse. A culture that shows a large difference between the best and the worst score is easier to change because there is less consensus of what the culture should be like.

For example, the Banking sector bubble is found down to the right. This bubble is showing a small variation within the industry. Conversely, the Education sector also shows a small variation, but with a much worse security culture score. In this context, you would want your organization and industry to be in the lower right region of the chart.

At the top of the chart, we find two large bubbles. The one to the left is the catch-all category of Other, which consists of any organizations that do not fit into any of the industry sectors. A large variation is to be expected in a group like this. The other sector with a lot of variation is the Technology sector.

The Technology sector's security culture score, and the variability thereof, is indicative of two realities: 1) this sector tends to serve as a catch-all because many business are loosely classified as "Technology" and 2) numerous breaches over the past decades testify that this sector does not have a stellar track record of factoring security into its operations and products.

# Comparing Security Culture Scores Across Industries

The security culture score is a measurement that describes the overall security culture of an organization. By aggregating the scores of organizations in each industry, we can learn how each industry compares across the seven dimensions of security culture.

The best performers of security culture are Banking (76), Financial Services (76), Insurance (75), and Technology (75). These industries tend to be highly regulated in areas of financial risk management as well as cybersecurity and privacy obligations.

At the bottom, we find industries like Education (68), Transportation (70), and Energy & Utilities (71).

Education is the only industry that scores below 70. The Education sector is broad and employees within are only recently beginning to accept their exposure to cybersecurity threats. They are often highly educated, yet not accepting of the huge shift toward digitalization and the new threats that arise as a result. The recent COVID-19 pandemic forced many technology-resistant sectors to embrace and adapt. The Education sector was highly impacted by this pandemic. As such, it will be interesting to evaluate their progress in 2021 to see if their cybersecurity culture improves at pace with their technology adoption; or if their culture gap grows, resulting in an increased risk.

Security researchers and the media have noted for years that the security of many critical infrastructure facilities is concerning. We see that lag reflected here as well in the security culture score of 71 for Energy & Utilities. Such facilities can include power plants, nuclear facilities, oil and gas related production units and refineries. The critical nature of these areas requires a major shift in security culture.

It is interesting to note that sectors typically comprised of “knowledge worker” employees are ranking higher than industries that rely on more traditional manufacturing and production. Although this may be explained by the extended use of computers and information technologies by knowledge workers, it also begs the question: as digitalization spreads into even more industries, are these industries ready to meet the related cybersecurity and security culture challenges?

Other notable sectors struggling with security culture include Government, Legal, and Retail sectors. It is also clear that the Not for Profit / NGO sector is doing well. This may be due to the nature of their business model and the delicacy of the information some of these entities are handling.

In general, a score below 80 is considered moderate, and a score below 60 is poor to moderate. As a result, security culture scores should be improved by all industries. There are a few organizations that stand out. The best-in-class score is 86 (Government), and the worst score is an organization with a score of 50 (Other).

Figure: Comparing Security Culture Scores

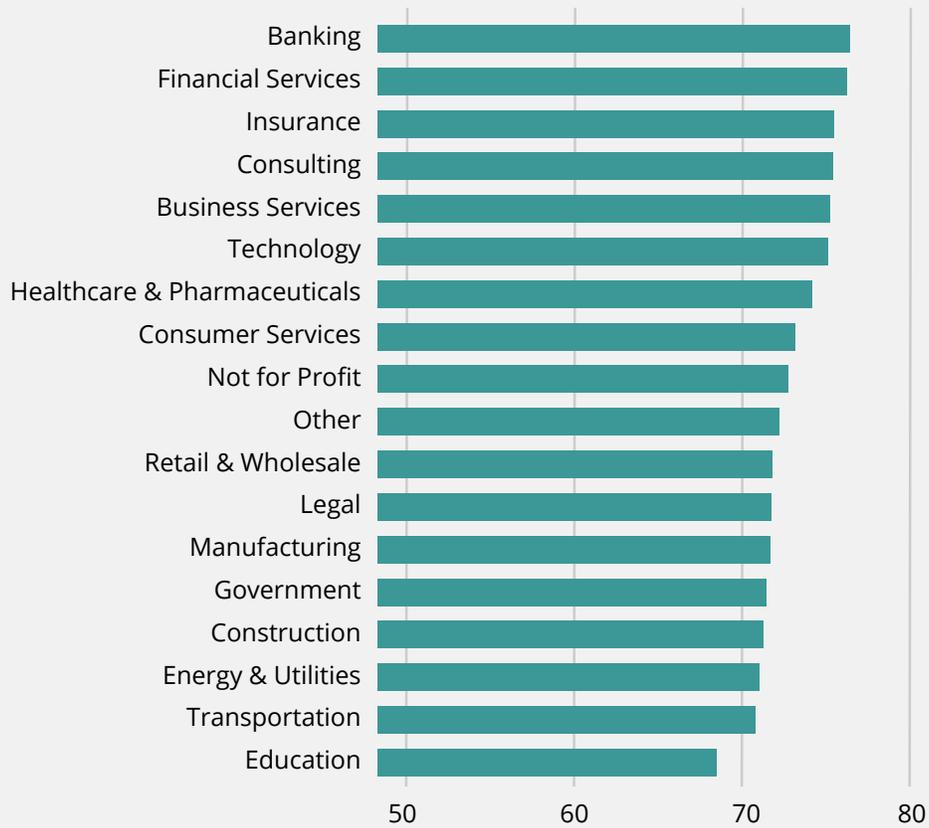


Table: Comparing Security Culture Scores

Industry	Score	Industry	Score
Banking	76	Healthcare & Pharmaceuticals	74
Business Services	75	Insurance	75
Construction	71	Legal	71
Consulting	75	Manufacturing	71
Consumer Services	73	Not for Profit	72
Education	68	Other	72
Energy & Utilities	71	Retail & Wholesale	71
Financial Services	76	Technology	75
Government	71	Transportation	70

## Comparing Attitudes

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

Exploring employee attitudes toward cybersecurity provides an important metric to help target awareness in a more proactive way. Attitudes are often conveyed with positive and negative terms, such as dislike, love, and prefer. Attitudes are major drivers for change in culture. As such, the higher the score on this dimension, the easier it will be to implement and manage security-related topics in an industry.

All industries have some challenges with attitudes. Banking, with a security culture score of 80, is the only industry with a good rating in the Attitudes dimension. All other industries have a moderate score in Attitudes, possibly leading to difficulties in transforming the organization toward a more secure culture.

The industry with the least favorable attitudes toward security is Education (73). With the ever-increasing use of computers, tablets, and other digital devices, it is important for this industry to educate itself on the risks and the steps necessary to protect itself. Following Education is Construction (74), Transportation (74), and Government (74). Poor attitudes lead to negativity and negligence toward security and must be addressed properly to reduce risk. Disgruntled employees turn into insider threats. Lack of training and education results in employees who do not understand the importance of security, and thus do not care about it.

Promoting a strong security culture is a management responsibility and should be made a priority. Proper prioritization can easily be detected by reviewing budgets/funding, how security products and services are sourced, and how proactive an organization is at managing security culture, including measuring and educating employees.

As with the old saying, “Do as I say, not as I do,” attitudes trickle down from the top. Having policies in place is a starting point. But ensuring that policies are also followed by the management team and that security is spoken about in a positive manner is key to managing a good security culture.



Figure: Comparing Attitude Scores

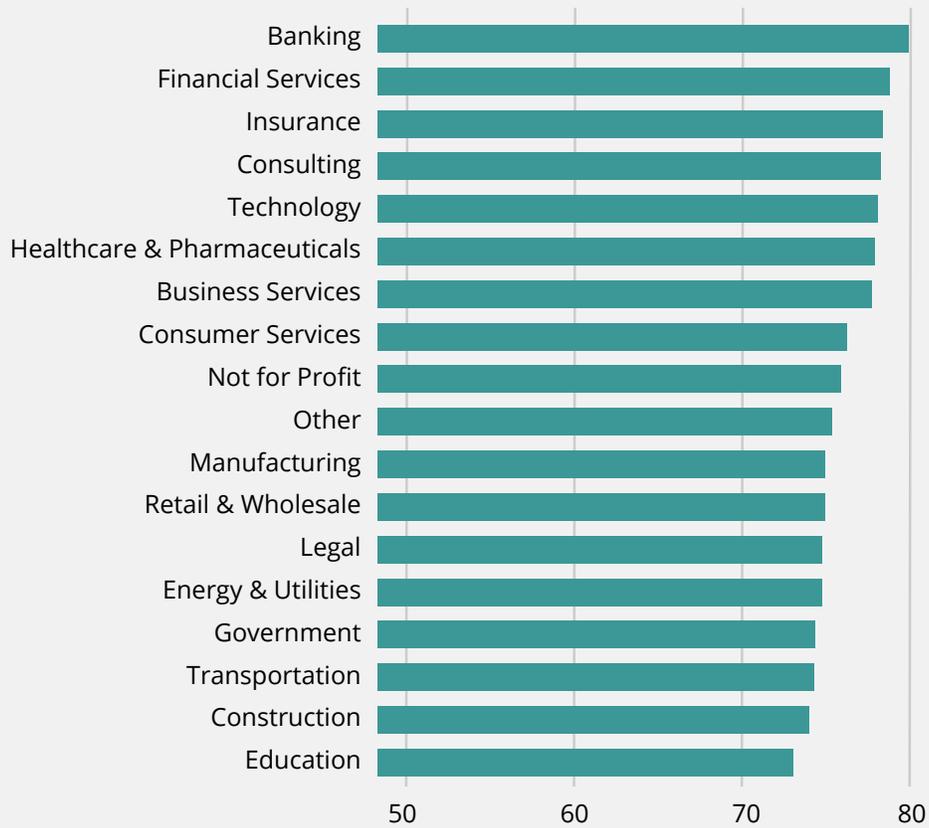


Table: Comparing Attitude Scores

Industry	Attitude	Industry	Attitude
Banking	80	Healthcare & Pharmaceuticals	78
Business Services	78	Insurance	78
Construction	74	Legal	74
Consulting	78	Manufacturing	75
Consumer Services	76	Not for Profit	76
Education	73	Other	75
Energy & Utilities	74	Retail & Wholesale	75
Financial Services	79	Technology	78
Government	74	Transportation	74

## Comparing Behaviors

*Behaviors: The actions and activities of employees who have direct or indirect impact on the security of the organization.*

Driving secure employee behavior is often the ultimate goal of security awareness programs. After all, there is usually a direct link between someone making a sound security decision (behavior) and security breaches and incidents. Industries with a high score on the Behaviors dimension have a low risk of insider threats <sup>[8]</sup>.

The Banking (78) industry is scoring higher than other industries. This may be due to the industry's long history of regulatory oversight, heightened risk management practices, and decades of training and education. It is followed by the Financial Services (76) and Insurance (76) sectors, which have similar histories.

Again, trailing the pack, we find Education (67). The near constant stream of security incidents reported in this sector may be explained by this lack of secure behaviors. Another poorly performing industry is Energy & Utilities (70). This is a sector that includes critical infrastructure like energy production and distribution, as well as water treatment plants. As critical infrastructure, they are expected to exercise above-average security. Their low score is notable, and we look forward to seeing how they address this deficit in the future.

All industries fall in the *moderate* security culture range, suggesting a need to improve behaviors. Behavioral change can be driven by improving the other six dimensions of security culture. The Norms dimension shows correlation with Behaviors: stronger norms are connected to improved behaviors.



Figure: Comparing Behavior Scores

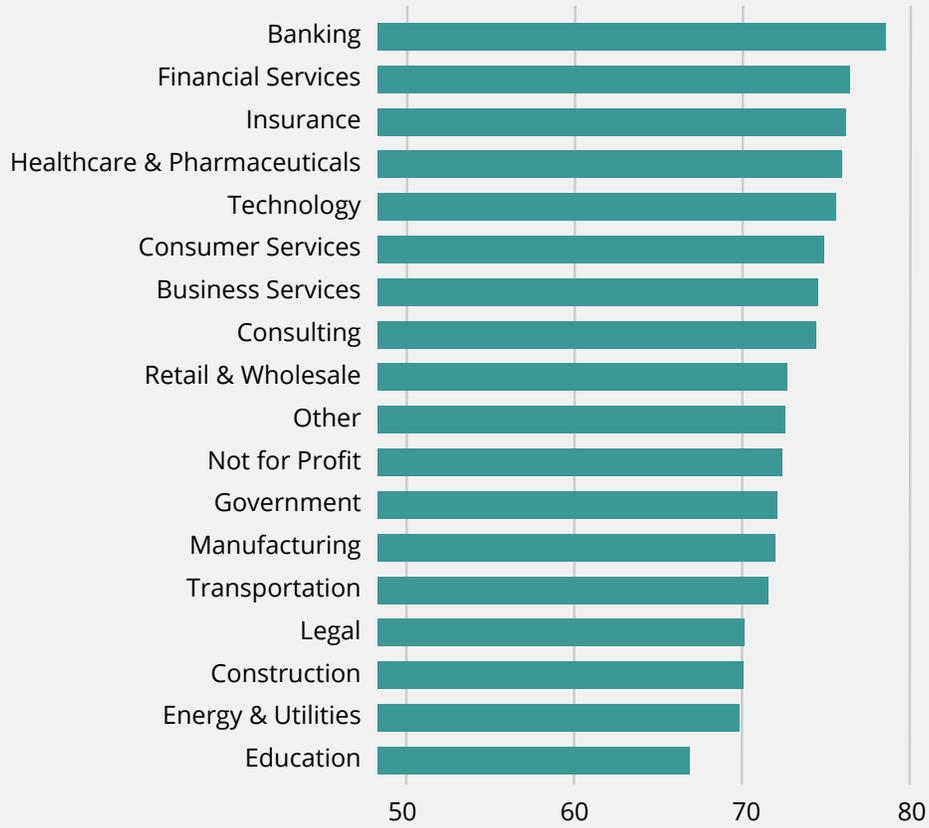


Table: Comparing Behavior Scores

Industry	Behavior	Industry	Behavior
Banking	78	Healthcare & Pharmaceuticals	75
Business Services	74	Insurance	76
Construction	70	Legal	70
Consulting	74	Manufacturing	72
Consumer Services	75	Not for Profit	72
Education	67	Other	72
Energy & Utilities	70	Retail & Wholesale	72
Financial Services	76	Technology	75
Government	72	Transportation	71

## Comparing Cognition

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

This dimension is a window into how well employees understand security-related issues and practices and how they apply their knowledge. Information-based security awareness and training is only helpful if the employees internalize it and then act on it; as such, the Cognition dimension is closely linked with the Responsibilities and Communication dimensions<sup>[9]</sup>.

All industries report moderate scores in the Cognition dimension. The industry that scores the highest is Technology (73), closely followed by Consulting (72), Financial Services (72), Banking (72), Business Services (72), and Insurance (71). These sectors have been highly exposed to the cyber domain and security-related information for a long time. It is often thought that because of their early adoption of technology, high regulatory scrutiny, and mature understanding of risk, they are also better at understanding and managing cybersecurity threats. As we show in this report, this is not entirely true. A score in the low 70s is not at all where it should be.

Education (66) is, again, at the bottom of the list. Ironically, the Education sector is the worst performing when it comes to learning, understanding, and managing security. The Energy & Utilities (66) industry is also performing extremely poorly. This industry includes critical infrastructure and should be focusing much harder on educating and assessing its employees.

With these moderate scores in Cognition, it will take considerable effort to reach acceptable levels for any of the industries. Implementing better training and education programs for employees across all industries is required. This should be combined with assessments, targeted interventions, and positive reinforcement. Executives should see this as a management responsibility. They should allocate funding and demonstrate good practice.

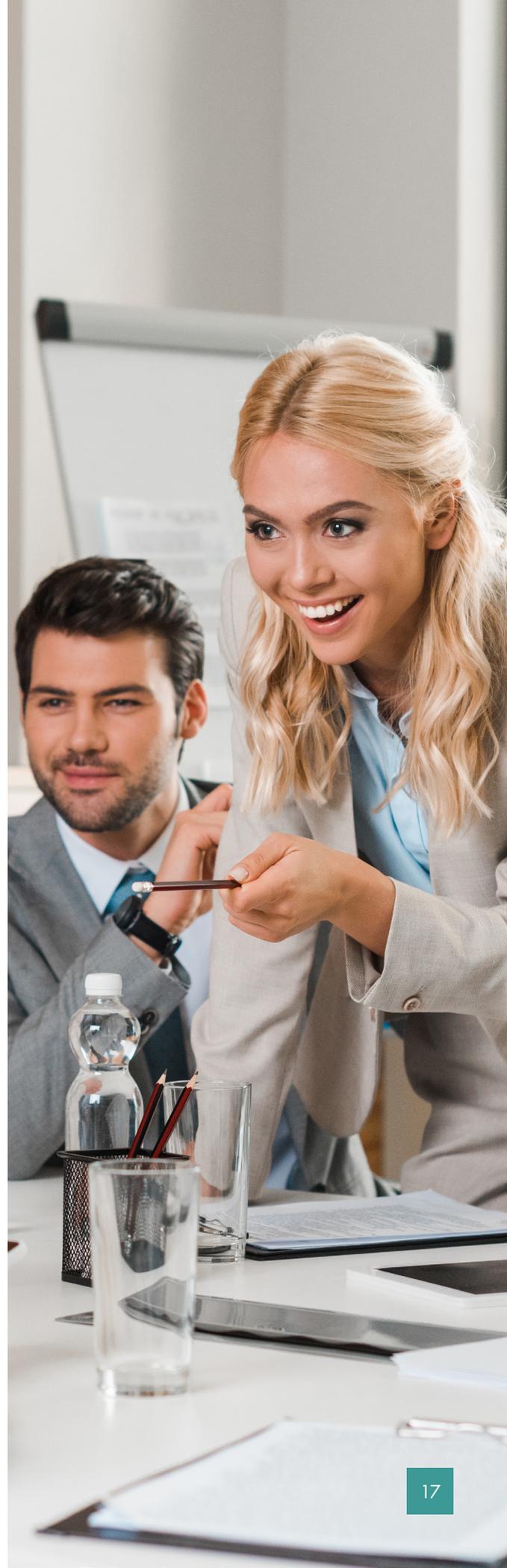


Figure: Comparing Cognition Scores

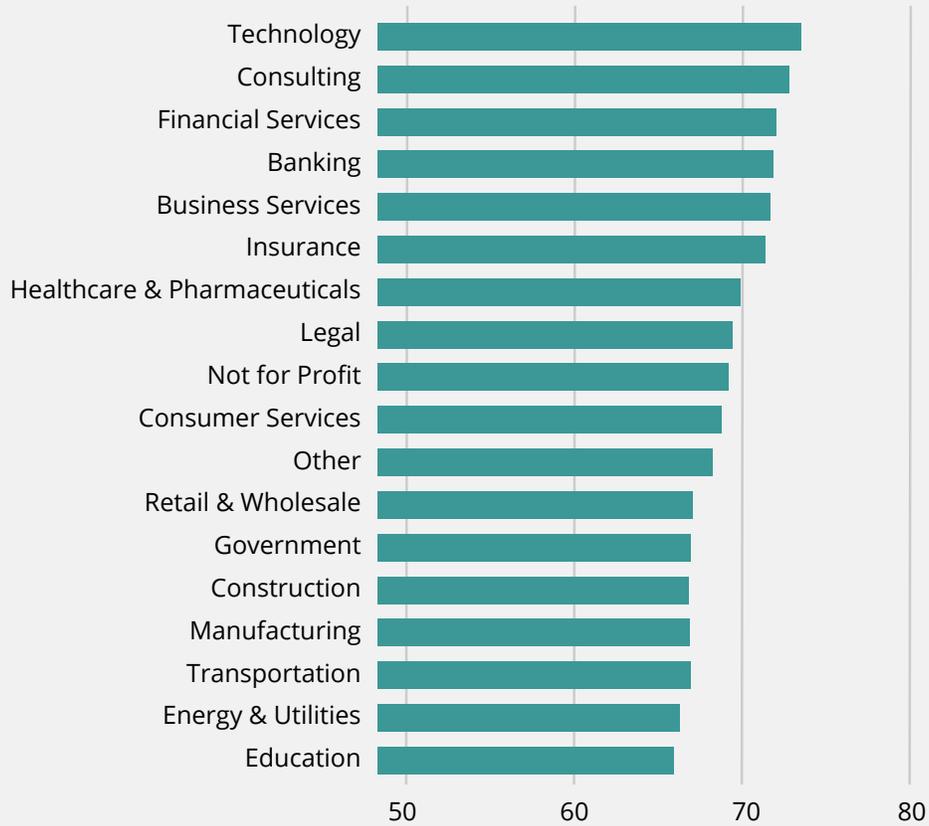


Table: Comparing Cognition Scores

Industry	Cognition	Industry	Cognition
Banking	72	Healthcare & Pharmaceuticals	70
Business Services	72	Insurance	71
Construction	67	Legal	69
Consulting	72	Manufacturing	67
Consumer Services	69	Not for Profit	69
Education	66	Other	68
Energy & Utilities	66	Retail & Wholesale	67
Financial Services	72	Technology	73
Government	67	Transportation	67

## Comparing Communication

---

*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.*

---

Some examples of characteristics indicating an excellent score in this dimension include using a variety of communication channels, frequent communication, and knowing when and to whom to provide relevant, security-related information.

The best performers in the Communication dimension are Financial Services (80) and Business Services (80), which barely scored in the good security culture bracket. They are closely followed by Consulting (79), Banking (79), and Insurance (79), which lie within the moderate bracket. All these sectors are well versed in communicating risk and security. They also share that they tend to operate across multiple industries, which may lead to a more open communication style.

Education (73), Transportation (75), and Government (75) struggle in this dimension, as they have in others.

Communicating security positively is critical for organizations. Make sure to focus on setting good examples and repeating the message over and over, as these factors seem to be the most effective. Use storytelling techniques, brand your messages, and link your campaigns to larger organizational initiatives where possible. Encourage employees to talk about security, both the negatives and the positives. This kind of communication and transparency makes it easier to monitor the organization and react to issues quickly.

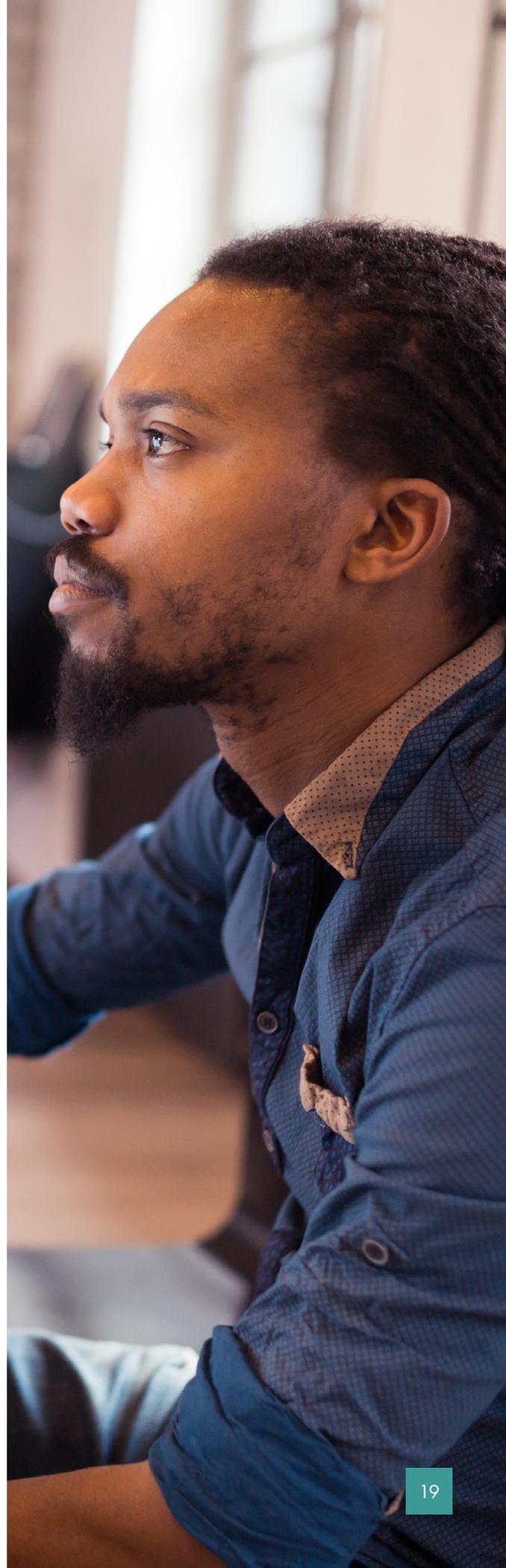


Figure: Comparing Communication Scores

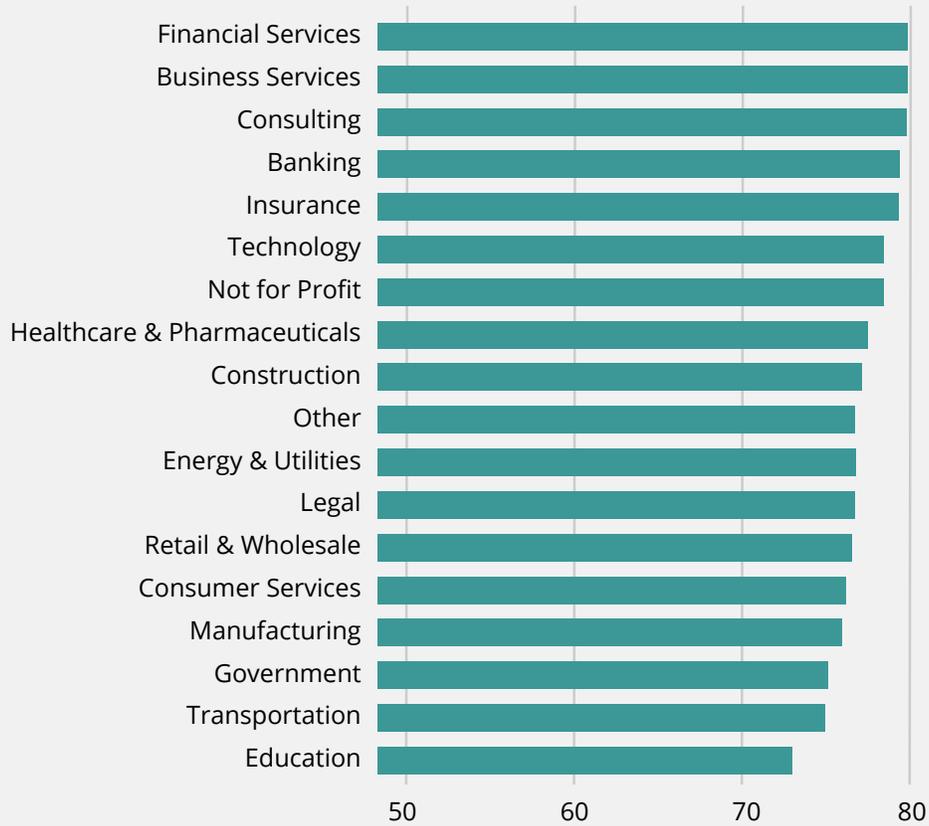


Table: Comparing Communication Scores

Industry	Communication	Industry	Communication
Banking	79	Healthcare & Pharmaceuticals	77
Business Services	80	Insurance	79
Construction	77	Legal	76
Consulting	79	Manufacturing	76
Consumer Services	76	Not for Profit	78
Education	73	Other	76
Energy & Utilities	76	Retail & Wholesale	76
Financial Services	80	Technology	78
Government	75	Transportation	75

## Comparing Compliance

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

To ensure high compliance rates, policies should be easily available, well-documented, and clearly understood. Employees should know how each policy affects them and their role. The Compliance dimension can be positively influenced by improving the quality of Communication, Norms, and Attitudes<sup>[10]</sup>.

In the Compliance dimension, it's predictable that the top performers will have a history of being highly regulated. Consistent with that prediction, Banking (79), Financial Services (77), and Insurance (77) claim the top spots. Most industries are clustered between 75 and 79, signaling strongly that compliance is considered important and relevant.

Despite having a reputation for fostering a 'check the box' mindset, the fact that most industries that scored highest in this dimension are highly regulated proves that regulation can positively improve security.

Education (67) again falls to the bottom of the list. Alarming, this is the only industry rating below 70. It is difficult to explain why an industry like Education is consistently scoring so poorly. This can't be attributed to a lack of educational potential, intellectual capacity, or by lack of policies and regulatory controls. Perhaps one reason is the solitude and independence indicative to the working environment of some teachers. Perhaps it is that highly educated people resent being 'preached at' and told what to do. Perhaps teachers care more about educating their pupils than to stay current themselves. One thing is certain: the Education sector must address this soon. Allowing this disconnect and becoming complacent with mediocrity should be seen as the antithesis of the educational ethic.

The key to improving compliance is to explain why the policy is in place and how it impacts each employee's workday. Create training programs that not only explain the content of the policies, but also the intent. Encourage dialogue and commitment. Running table-top exercises and playing "what if" games can be helpful in communicating the intent and impact of policies, regulations, and security-related issues.

10 Research paper by CLTR: The Seven Dimensions of Security Culture



Figure: Comparing Compliance Scores

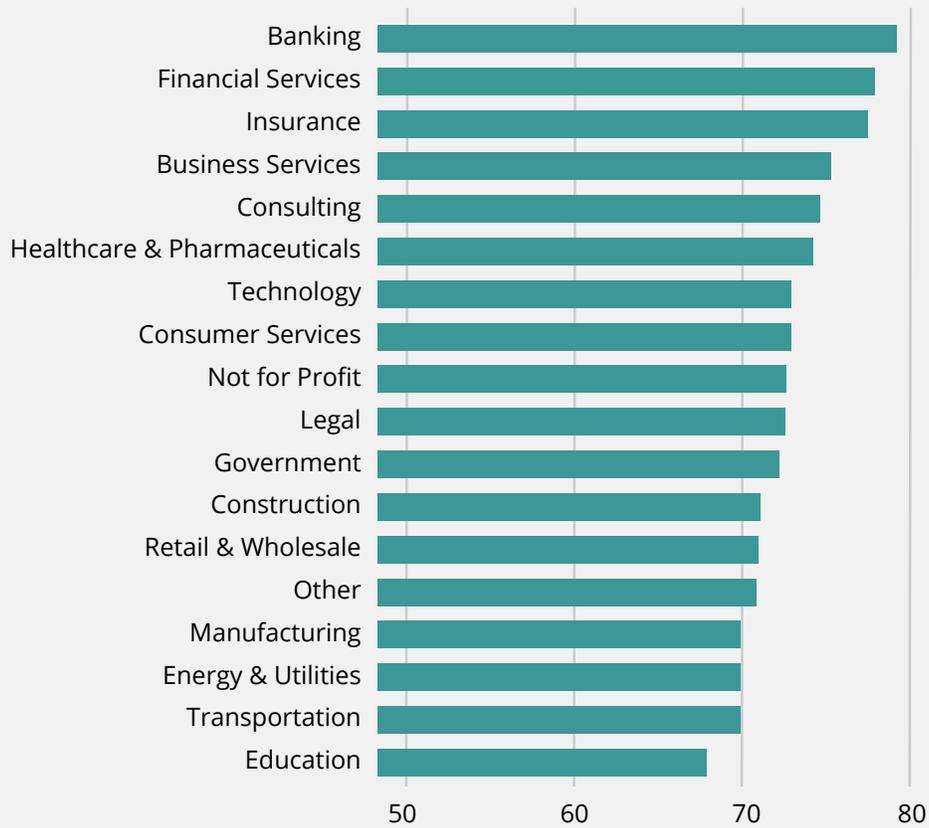


Table: Comparing Compliance Scores

Industry	Compliance	Industry	Compliance
Banking	79	Healthcare & Pharmaceuticals	74
Business Services	75	Insurance	77
Construction	71	Legal	72
Consulting	74	Manufacturing	70
Consumer Services	73	Not for Profit	72
Education	67	Other	71
Energy & Utilities	70	Retail & Wholesale	71
Financial Services	77	Technology	73
Government	72	Transportation	70

## Comparing Norms

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

Norms are behaviors that are modeled by others and become the implicit standard. For example, if having a no-tailgating habit is the norm, it would be considered normal and acceptable to not hold the door open for people you do not know. On the other hand, if the norm is to let anyone into the building, it would be considered unusual to stop people at the door. CLTRe research has shown that there is a strong correlation between the dimensions Behaviors and Norms<sup>[11]</sup>. Norms create social pressures and expectations.

All industry sectors fall well within the moderate bracket of the security culture index. The best industries, Business Services (73), Technology (73), and Financial Services (73), are likely on top due to their decades-long efforts to train employees. As such, some behavioral expectations and security-related knowledge have become ingrained. Unfortunately, even though these industries are at the top of the pack, they fall short from the next bracket that starts at 80.

Education (66) again trails other industries, followed closely by Legal (67). The low score in these industries shows that cybersecurity-related values have not yet valued or enculturated in these industries. Education and Legal should put an extra focus on developing strong norms before they fall even further behind other industry sectors.

Improvements are needed across all industries to reach a good score on Norms. Industries should focus on creating campaigns advocating for information security norms and keeping internal channels open to reward and share best practices. It is also extremely important to model the behaviors that you want employees to adopt as normative. Having security champion (aka “culture carrier”) programs can help as well.

---

11 Research paper by CLTRe: The seven dimensions of security culture



Figure: Comparing Norm Scores

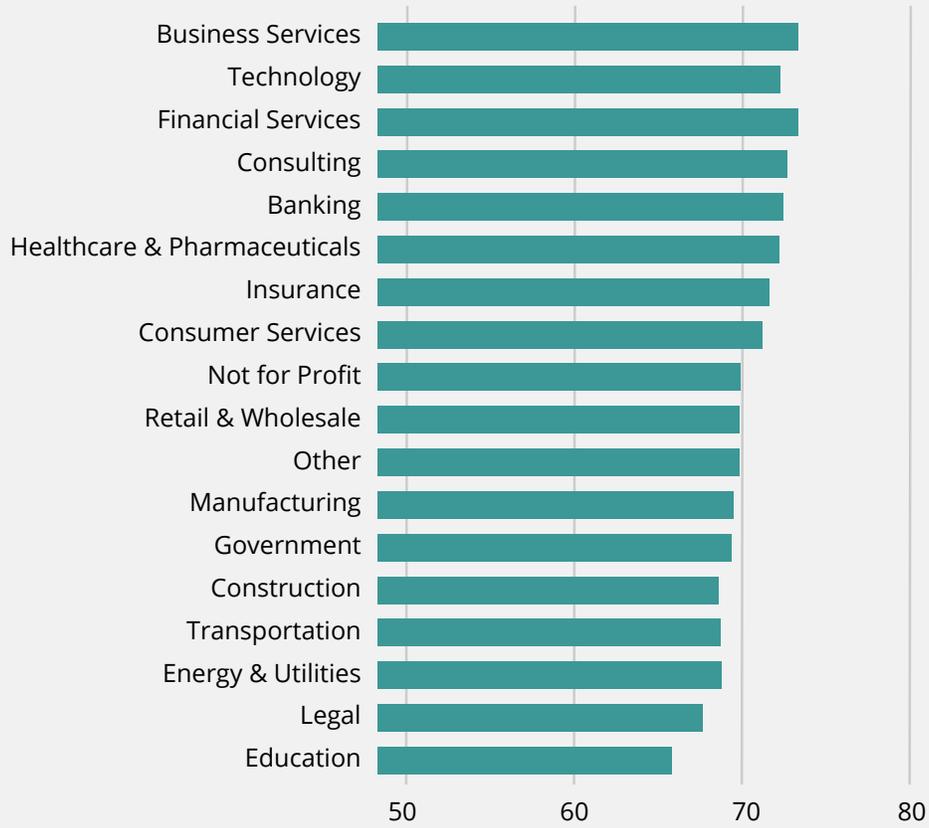


Table: Comparing Norm Scores

Industry	Norms	Industry	Norms
Banking	72	Healthcare & Pharmaceuticals	72
Business Services	73	Insurance	71
Construction	68	Legal	67
Consulting	72	Manufacturing	69
Consumer Services	71	Not for Profit	70
Education	66	Other	69
Energy & Utilities	68	Retail & Wholesale	69
Financial Services	73	Technology	73
Government	69	Transportation	68

## Comparing Responsibilities

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

This dimension is strongly related to practices and performance. Part of achieving an excellent score for Responsibilities is getting everyone in the organization to understand that security is their responsibility.

The industries scoring the highest are Banking (74), Consulting (73), Financial Services (73), Business Services (73), and Technology (73). High scores in these industries are not surprising, as they have been global targets of cybercrime and social engineering for decades. These industries have also historically taken steps in the right direction by training their employees and communicating security risks to them. However, all industries fall well within the moderate bracket, indicating that there is a need for improvement throughout all industry sectors.

Education (67) again finds itself in the bottom spot, with Transportation (68) and Government (69) performing only slightly better. Compared with the highest-ranking sectors, these are industries that have only recently started considering and acting to prevent social engineering and cybercrime. With the constant increase in cybercrime, there is an urgent need for these industries to improve.

Improvement can be achieved through an intentional focus on addressing employees' understanding of their critical role in helping to secure their organization. One multifaceted way of increasing employees' understanding is by conducting security awareness training, frequent social engineering testing, and by management's consistent messaging and modeling of the importance for everyone to do their part. Finding training content that considers all employees to be the last line of defense is essential. With increased knowledge and awareness, it is more likely that employees will begin to embrace security-related values and shift their behaviors accordingly.



Figure: Comparing Responsibilities Scores

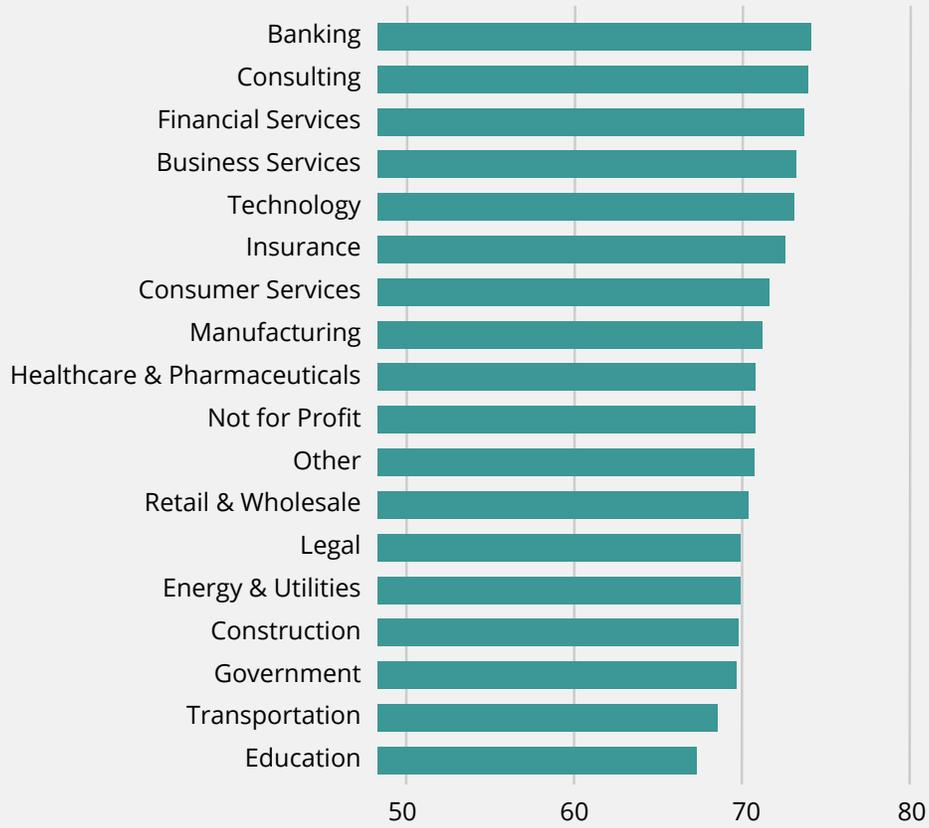


Table: Comparing Responsibilities Scores

Industry	Responsibilities	Industry	Responsibilities
Banking	74	Healthcare & Pharmaceuticals	71
Business Services	73	Insurance	72
Construction	69	Legal	69
Consulting	73	Manufacturing	71
Consumer Services	71	Not for Profit	70
Education	67	Other	70
Energy & Utilities	69	Retail & Wholesale	70
Financial Services	73	Technology	73
Government	69	Transportation	68

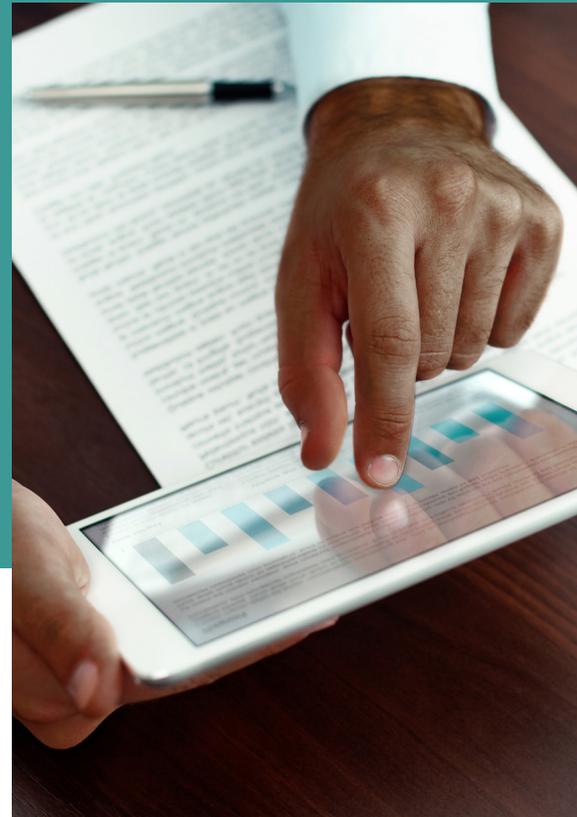
# Industry Benchmark

In this section of the report, 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.

## How to Read the Industry Page

Each industry sector has its own description, data table, and graphs. Find the industry you are interested in and get a quick glance of the industry score on the top right of the first page. That number represents the benchmark score. Just beneath the score itself are two data points: the number of organizations in our sample and the number of respondents in our sample.

Read the description for our analysis of the industry, as well as our industry-specific recommendations, called areas for improvements. On the opposite page of the descriptions, you can find the data we used in different formats: tabular data as well as graphs to visualize the results. The two graphs we use are explained below.



### 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 whiskers sticking out from the box. The bottom whisker indicates where the lower 25% of the scores fall, and the upper whisker indicates

where the top 25% of the scores fall. The end point of the whiskers, where the dotted line stops with a horizontal line, indicates the minimum and maximum scores. You might also see some circles on the plot, which are outlier scores, that are very different from the others.

### How to Read the Column Chart

Column charts use columns to show the comparison between categories or things. 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.

### 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 six levels that explain the quality of the security culture.

The security culture index levels are:

- 90-100** Excellent
- 80-89** Good
- 60-79** Moderate
- 50-59** Poor to moderate
- 30-49** Poor
- 0-29** Extremely poor

# Banking

The Banking sector has a long tradition of managing risk across many areas. The experience and understanding of risk management is showing a faster and more thorough adoption of cybersecurity, including early adoption of employee training. The proactive risk management strategy is providing the banking sector with a reasonably good security culture score of 76.

Employee survey results within the Banking sector reflect strong, positive attitudes toward security. With a score of 80 in the Attitudes dimension, it is likely that employees in this sector feel positive toward making behavioral, procedural, or technology-related adjustments as required and adopting security practices.

Furthermore, we see that communication is a crucial part of building security culture. In the Banking sector, the Communication dimension is at 79. There are good information channels available to employees that allow them to access the right information easily and effortlessly at the right time. The Banking sector is also strong on adherence to policies. With a Compliance score of 79, employees are well informed of the policies and follow them quite well.

This strong positivity is further reflected in the security behaviors of the employees. The Behaviors dimension looks at how employees behave regarding security, and this dimension rates at 78 points.

## Areas for Improvement

The Banking sector is showing poor performance in the Norms dimension, with a score of 72. This dimension measures the unwritten rules related to security expectations and how employees are adopting them. There is a strong connection between Behaviors and Norms (SCR2017), and the banking sector is likely to see direct improvement on Behaviors by improving the Norms dimension.

Employee knowledge and competence is critical in a successful risk management program.

This is one area where the banking sector can improve. A score of 72 in the Cognition dimension is a clear indicator that there is a need for improved training and education programs. The strong positive attitudes toward security show that employees within this sector are extremely likely to embrace quality training, especially when they understand the benefits of doing so.



# Statistics for Banking

Bar Plot: Score for All Dimensions in Banking



Table: Means per Dimension

Dimension	Mean	Dimension	Mean
Attitudes	80	Compliance	79
Behaviors	78	Norms	72
Cognition	72	Responsibilities	74
Communication	79	Security Culture Score	76

Box Plot: Security Culture Score for Banking



Table: Total Number of Completed in Banking

Industry	Number of Employees
Banking	10,873

Table: Descriptive Statistics

Min	25%	Mean	Median	75%	Max
68	74	76	76	78	86

## Business Services

Organizations within the Business Services sector typically offer assistance in areas such as office administration, security, garbage disposal, cleaning services, and hiring and placing personnel, just to name a few. This industry houses a large variety of organizations offering differing services, making for an interesting mix in overall measurement of descriptive statistics. This industry is specifically prone to a high percentage of targeted phishing attacks (Source: KnowBe4 Phishing by Industry Benchmarking Report 2020). Across small, medium, and large Business Services organizations, there is a high rate of susceptibility to being compromised, indicating a higher risk level.

The Business Services sector shows a favorably healthy attitude toward security and a willingness to take appropriate measures to better secure their organizations. A score of 78 in the Attitudes dimension shows that employees demonstrate a moderate eagerness to be compliant with security measures. Additionally, a good Communication dimension score of 80, 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 moderate Compliance score, 75, indicates 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 Cognition score of 72, we see that although employees demonstrate an eagerness to be compliant with security measures as indicated above, the industry needs to have a higher dedication to providing meaningful and ongoing security awareness training for all employees.

Additionally, with scores of 73 each, the areas of Norms and Responsibilities are also reflected as moderate. A significant improvement in 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.



# Statistics for Business Services

Bar Plot: Score for All Dimensions in Business Services

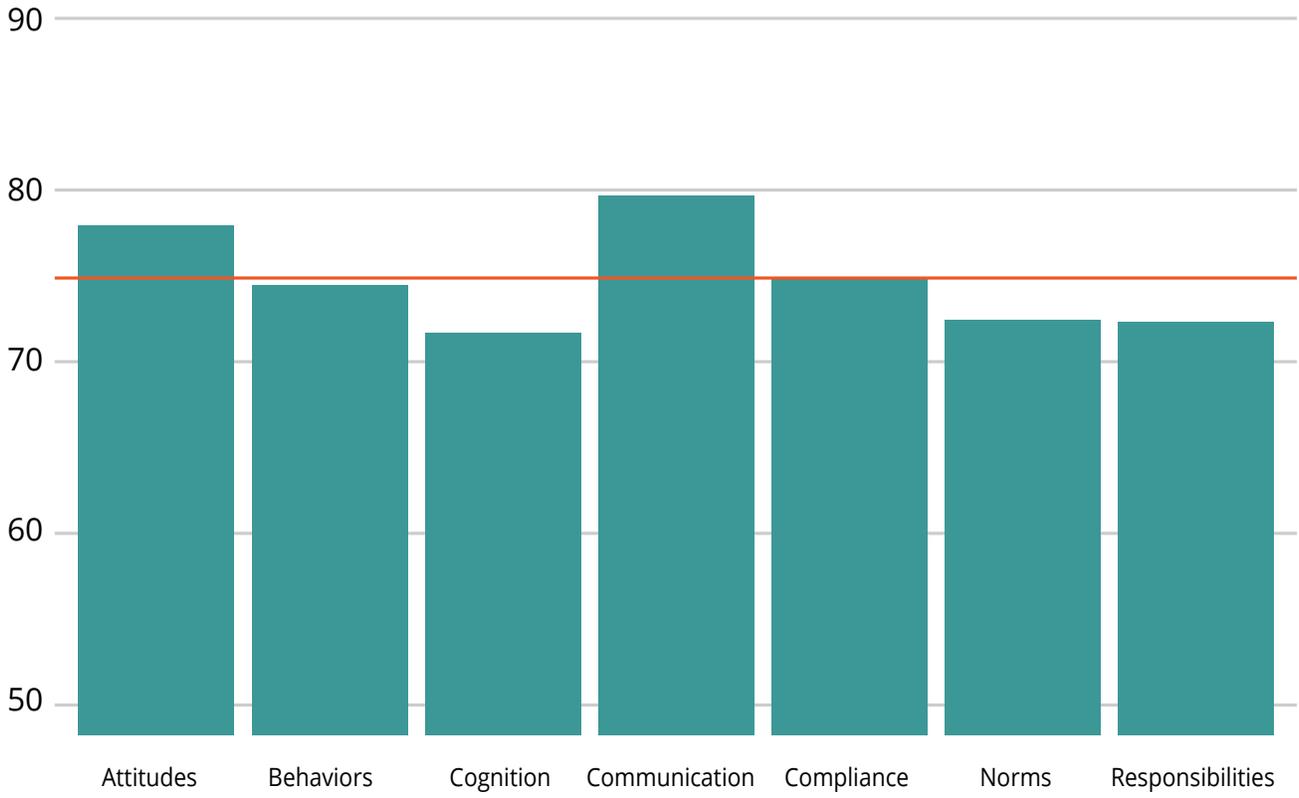


Table: Means per Dimension

Dimension	Mean	Dimension	Mean
Attitudes	78	Compliance	75
Behaviors	74	Norms	73
Cognition	72	Responsibilities	73
Communication	80	Security Culture Score	75

Box Plot: Security Culture Score for Business Services



Table: Total Number of Completed in Business Services

Industry	Number of Employees
Business Services	2,799

Table: Descriptive Statistics

Min	25%	Mean	Median	75%	Max
64	72	75	75	78	85

## Construction

The Construction industry, which often includes a complex structure of contractors, engineers, and skilled tradesmen, has long been a healthy target for cyber criminals. With such a complex structure comes even greater complications in the private exchange of information and currency. Mid-size Construction organizations have been among the most targeted and susceptible to phishing attacks overall, (Source: KnowBe4 Phishing by Industry Benchmark Report 2020), as well as earning some of the lowest security culture-related ratings in this research.

The most favorable score for the Construction industry is shown through their ability to communicate, a moderate 77. This score shows that there is a reasonable approach to communicating with employees across their challenging structures. But because of their underlying framework, they need to pay close attention to the kinds of messaging being directed at each audience and the mediums through which they communicate. Targeted communications focusing on the unique, security-related threats, issues, and responsibilities for each role will increase.

### Areas for Improvement

The most significant area for improvement within the Construction industry is in Cognition. The score of 67 in this dimension, while considered moderate, indicates that there is much work to be done. 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, which is not generally considered a viable option.

The Construction industry is also struggling in the dimensions of Norms (68) and Responsibilities (69). Without an appropriate structure 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. Additionally, employees may mistake unacceptable security-related behaviors as acceptable because there is a lack of understanding of what proper conduct looks like.



# Statistics for Construction

Bar Plot: Score for All Dimensions in Construction



Table: Means per Dimension

Dimension	Mean	Dimension	Mean
Attitudes	74	Compliance	71
Behaviors	70	Norms	68
Cognition	67	Responsibilities	69
Communication	77	Security Culture Score	71

Box Plot: Security Culture Score for Construction



Table: Total Number of Completed in Construction

Industry	Number of Employees
Construction	4,447

Table: Descriptive Statistics

Min	25%	Mean	Median	75%	Max
61	68	71	71	73	77

# Consulting

Consulting firms are very attractive targets for cyber criminals. They are data rich. With data ranging from intellectual property, financial information, to strategic planning, growth strategies, gap analysis studies, and more, these firms are consistently high-profile targets. Clients of Consulting firms expect elevated levels of confidentiality, which may prove challenging with the high-paced and stressful environment generally bred in this industry.

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 show very positive trends towards becoming more secure through Attitudes (78) and Communication (79). Within the Consulting sector, it is highly likely that employees understand their respective roles and responsibilities and will readily make appropriate adjustments to adopt more favorable security practices. Additionally, with a moderately high score in the Communication dimension, it is probable that Consulting firms lean on consistency and clarity in authoring messaging and the outcomes expected because of those messages.

## Areas for Improvement

With a score of 72, Consulting firms show a moderately low score on the Cognition dimension. It is likely that as 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 72 for Norms is moderately low, revealing that Consulting firms need 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." (Source: The 7 Dimensions of Security Culture).



# Statistics for Consulting

Bar Plot: Score for All Dimensions in Consulting

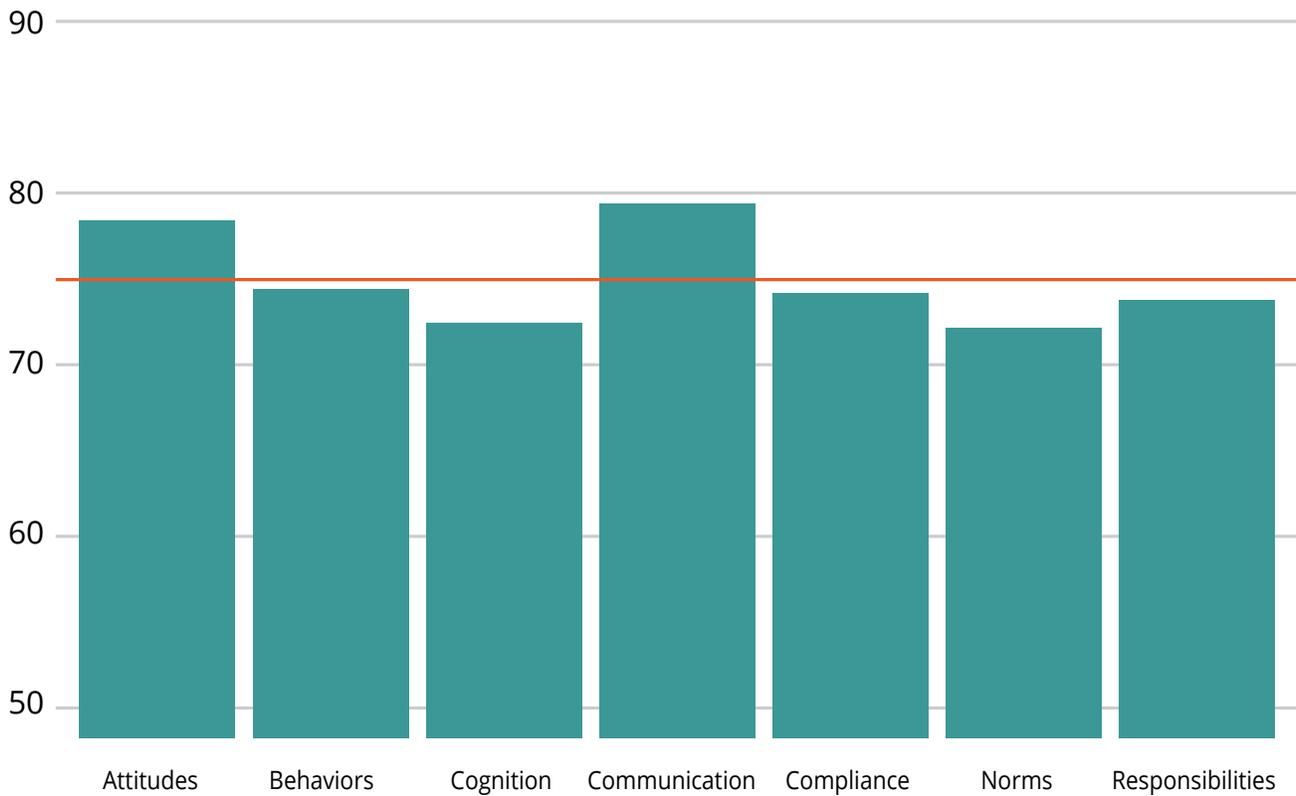


Table: Means per Dimension

Dimension	Mean	Dimension	Mean
Attitudes	78	Compliance	74
Behaviors	74	Norms	72
Cognition	72	Responsibilities	73
Communication	79	Security Culture Score	75

Box Plot: Security Culture Score for Consulting

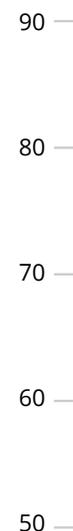


Table: Total Number of Completed in Consulting

Industry	Number of Employees
Consulting	1,429

Table: Descriptive Statistics

Min	25%	Mean	Median	75%	Max
66	73	75	75	78	82

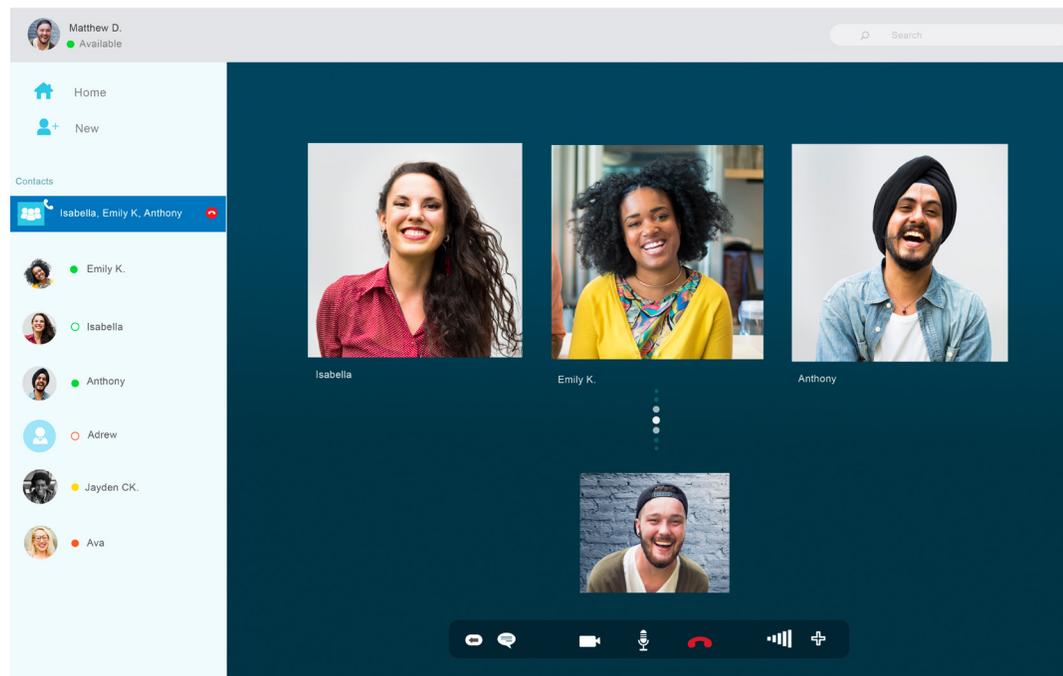
# Consumer Services

Organizations in the Consumer Services sector typically offer support-based products that are not physical in nature. This industry houses a large variety of organizations that offer differing services, making for an interesting mix in overall measurement of descriptive statistics.

The Consumer Services sector has long been challenged with keeping up with technological advances that would help to reinforce their security infrastructures. Prone to mischief in the forms of identity theft and credit card fraud, organizations in this sector are challenged in getting ahead of the criminals through strengthening of their human firewalls.

With moderately high scores in the Attitudes and Communication dimensions, both 76, we understand “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). In this case, Consumer Services organizations can use communications internally to positively impact the attitudes of their employees, and externally to drive trust and confidence through their customer base.

If employees have a continuous flow of information targeted specifically at raising their security acumen, they will be better positioned to protect and defend the organization, should a risk arise. When consumers believe that the organization is guarding their personal information and taking the appropriate steps to mitigate any potential risk, it is likely they will maintain a long buyer/seller relationship with that organization.



## Areas for Improvement

The dimension of Cognition had a moderate score of 69. With a more dispersed pool of talent, Consumer Services organizations are challenged to ensure that there is consistent security understanding across their employees. Consumer Services organizations that implement strong, well-designed, security training programs for incoming talent are positioned with a strong foundation from which to build.

Two additional dimensions that reflected moderate scores of 71 were Norms and Responsibilities. Consumer Services sector organizations are struggling to establish solid norms due to their diverse and 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. Norms can be improved by more intently focusing on Communication and Attitudes while evangelizing (using communication and positive recognition) proper security-related behaviors.

# Statistics for Consumer Services

Bar Plot: Score for All Dimensions in Consumer Services

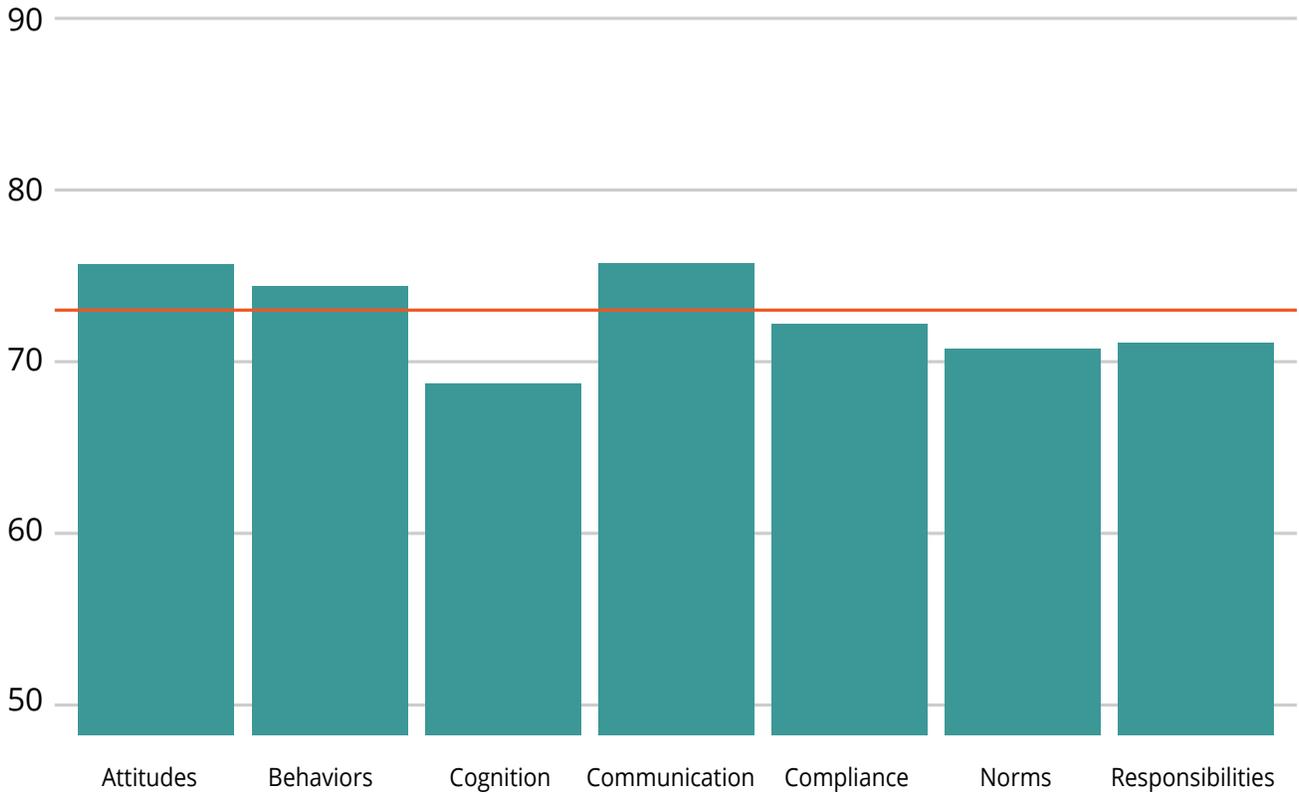


Table: Means per Dimension

Dimension	Mean	Dimension	Mean
Attitudes	76	Compliance	73
Behaviors	75	Norms	71
Cognition	69	Responsibilities	71
Communication	76	Security Culture Score	73

Box Plot: Security Culture Score for Consumer Services



Table: Total Number of Completed in Consumer Services

Industry	Number of Employees
Consumer Services	1,471

Table: Descriptive Statistics

Min	25%	Mean	Median	75%	Max
66	71	73	73	74	80

## Education

The Education sector often manages risk differently across public, private, and higher education institutions. This diversity of security and risk-related experience and understanding is exhibited by varying approaches to the adoption of cybersecurity; and is usually exasperated by limited funding. The security culture score of 68 falls in the moderate range. But even though the sector's score falls in the moderate range, we must unfortunately point out that the Education sector earned a last place ranking in each of our industry comparisons.

The Education sector is an increasingly attractive target for ransomware attacks enabled by successful phishing operations (Source: KnowBe4 Phishing by Industry Benchmark Report 2020).

The Education sector shows a moderate attitude toward security. With a score of 73 in the Attitudes dimension, it is likely that employees in this sector are average when making adjustments and adopting security practices, given the nature of their roles in Education. In the Education sector, the Communication dimension is at 73. There is a diversity of information channels available to employees in the various educational environments that allows them to access the required information at the right time.

### Areas for Improvement

With a Compliance score of 67, employees are only reasonably informed of the policies and on par with implementing practice of said policies. The Behaviors dimension looks at how employees behave regarding security, and this dimension rates at 67. Responsibilities also scored a 67.

Employee knowledge and competence is vital to successful security and risk management programs. This is another area where the Education sector can improve. The score of 66 in the Cognition dimension is a clear indicator that there is a need for improved training and education programs.

This sector also shows room for improved performance in the Norms dimension (also a 66). This dimension measures awareness of and adherence to unwritten rules. The identical score between Cognition and Norms indicates that the Education sector can experience direct improvement on Behaviors by improving the Norms dimension, which should improve by focusing on the Cognition dimension and by leveraging the stronger Communication (73) dimension.



# Statistics for Education

Bar Plot: Score for All Dimensions in Education

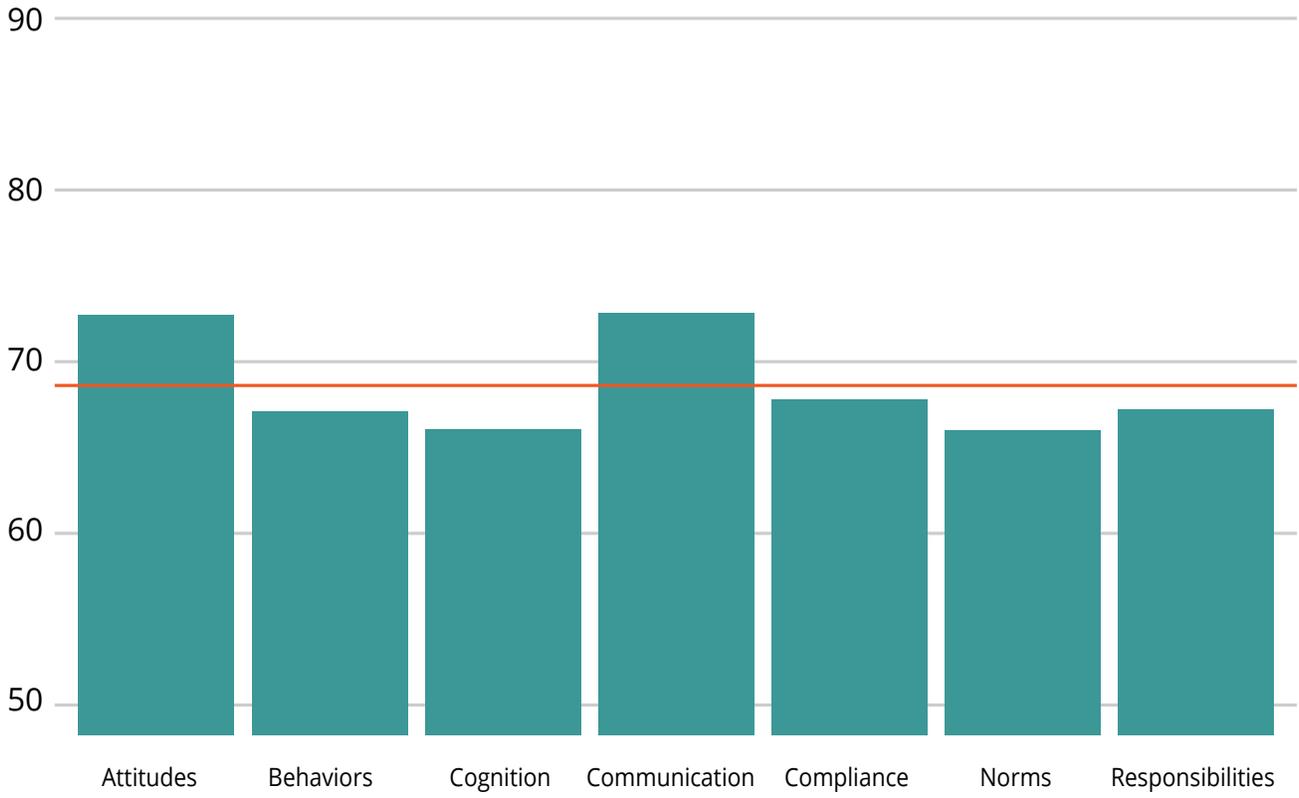


Table: Means per Dimension

Dimension	Mean	Dimension	Mean
Attitudes	73	Compliance	67
Behaviors	67	Norms	66
Cognition	66	Responsibilities	67
Communication	73	Security Culture Score	68

Box Plot: Security Culture Score for Education



Table: Total Number of Completed in Education

Industry	Number of Employees
Education	4,940

Table: Descriptive Statistics

Min	25%	Mean	Median	75%	Max
57	65	68	68	72	76

## Energy & Utilities

The Energy and Utilities sector, given the vital nature of their industry, faces an ongoing series of threats by nation states and cyber criminals alike. There are several federal and nonprofit entities focused on providing this sector with relevant security training, risk detection, and threat analysis tools. Despite these measures, the industry survey results earn them only a moderate security culture score of 71.

With a score of 74 in the Attitudes dimension, employees in this sector can improve in their understanding of the significance of their role in critical infrastructure and display greater willingness to implement and maintain security practices. The Communication dimension is at 76, indicating that the sector has adequate capabilities for providing relevant information to their employees. With a Compliance score of 70, employees are likely informed of compliance policies and how to follow them, but not in ways as effective or motivating as many other sectors. This is reflected in the security behaviors of the employees. The Behaviors dimension looks at how employees behave regarding security, and this dimension rates at 70 points. Responsibilities neared Compliance and Behaviors at 69. It is significant to note the similarity of scoring amongst Behaviors, Compliance, and Responsibilities— these dimensions strongly impact the role of overall security culture.

### Areas for Improvement

The Energy and Utilities sector shows moderate performance on the Norms dimension with a score of 68. This dimension is measuring the unwritten rules and how employees are adopting them. There is a strong connection between Responsibilities and Norms, and the Energy and Utilities sector will experience direct improvement on the Norms dimension as the role of employees' responsibility increases with ongoing security training.

The Cognition dimension scored lowest, at 66, and represents the greatest vulnerability for this sector. Limited cognition means limited employee resilience to social engineering tactics, providing an easy vector for cyber criminals to trick employees into allowing them access to vital data, while potentially enabling shorter attack timelines.



# Statistics for Energy & Utilities

Bar Plot: Score for All Dimensions in Energy & Utilities

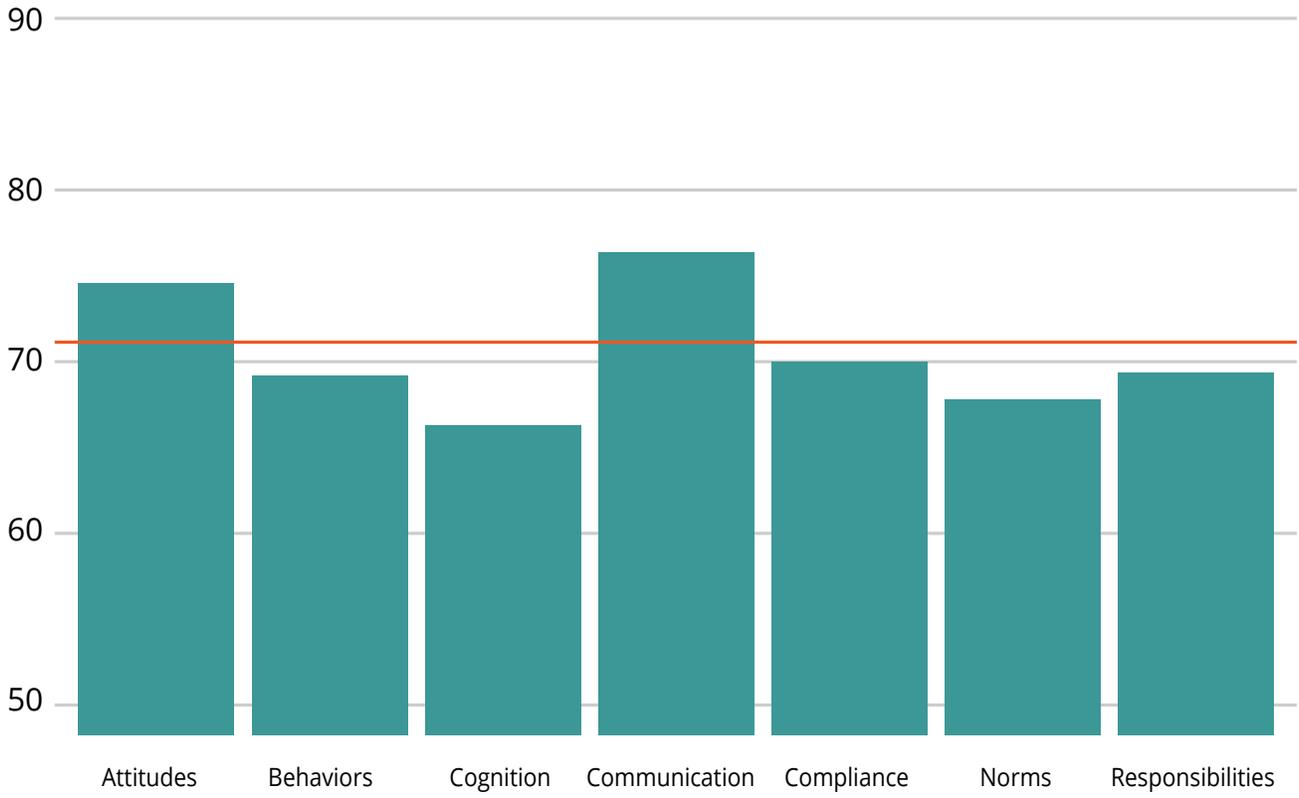


Table: Means per Dimension

Dimension	Mean	Dimension	Mean
Attitudes	74	Compliance	70
Behaviors	70	Norms	68
Cognition	66	Responsibilities	69
Communication	76	Security Culture Score	71

Box Plot: Security Culture Score for Energy & Utilities



Table: Total Number of Completed in Energy & Utilities

Industry	Number of Employees
Energy & Utilities	3,484

Table: Descriptive Statistics

Min	25%	Mean	Median	75%	Max
63	68	71	71	73	77

## Financial Services

The Financial Services sector has several years of experience managing and mitigating risk. When you control, trade, and govern significant amounts of money, all while housing highly confidential financial and personal client information, it is a given that you would be at the top of a cyber criminal's target list. 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.

Communication for Financial Services organizations scored in the good category at 80. Threats are quickly and ever evolving in this sector. Therefore, the ability to clearly communicate consistent messaging on emerging threats is critical. The messaging needs to be created and circulated in timely and relevant ways for each respective role in the organization. An inability to cascade useful and real-time information could lead to a crippling cyber attack that would cause both financial chaos and unforgiving reputational damage. Consider the attacks that befell Equifax, JPMorgan Chase or TRW Information Solutions. Each caused significant disruption and financial harm.

### Areas for Improvement

The Financial Services sector earned a moderate performance score in the Cognition dimension (72). 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). A comprehensive security training program will not only help to close the understanding gap, but it will also help to reinforce security-related best practices that should be top of mind for every employee.

We also recorded moderate performance for both Norms and Responsibilities, each at 73. This score in the Norms dimension is a clear indicator that while time is being spent on training to lift understanding, equal time needs to be invested in stimulating professional norms to help drive a stronger security culture and shared values. This also translates in the personal responsibility element and how employees see their own actions contributing to the security of the organization.



# Statistics for Financial Services

Bar Plot: Score for All Dimensions in Financial Services



Table: Means per Dimension

Dimension	Mean	Dimension	Mean
Attitudes	79	Compliance	77
Behaviors	76	Norms	73
Cognition	72	Responsibilities	73
Communication	80	Security Culture Score	76

Box Plot: Security Culture Score for Financial Services

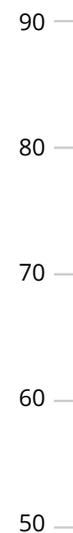


Table: Total Number of Completed in Financial Services

Industry	Number of Employees
Financial Services	10,146

Table: Descriptive Statistics

Min	25%	Mean	Median	75%	Max
65	73	76	76	78	84

## Government

The Government sector has extensive experience with managing risk across a vast and diverse enterprise, extending to both on-prem and cloud-based architecture. This experience includes an understanding of risk management, prompting an early recommendation of employee training (Source: NIST 800-50, yr. 2003). Despite these efforts, this sector earned only a moderate security culture score of 71.

Government sector organizations show questionable attitudes toward security and cybersecurity risks. With a score of 74 in the Attitudes dimension, it is likely that employees in this sector are moderately aware of the need to increase their security behaviors. The highest rated dimension was Communication (75), indicating that employees view their various communication sources as useful for obtaining relevant information.

Surprisingly, the Government sector scores worse on their adherence to policies. With a Compliance score of 72, employees are not entirely well informed of policies and, despite numerous compliance requirements throughout federal, state, and local governments, there is an ongoing opportunity for improvement in this area. The effects of this score are also reflected in the security behaviors of the employees. The Behaviors dimension looks at how employees behave regarding security, and this dimension rates at 72 points.

### Areas for Improvement

The Government sector showed moderate performance on the Norms dimension with a score of 69. This dimension measures understanding of an organization's unwritten rules and codes of conduct, and how employees are adopting them. The Responsibilities dimension also only scored a 69, demonstrating a lack of ownership to securing the organization.

Cognition is another area where the government sector can improve. The score of 67 in the Cognition dimension is the lowest of all dimensions. This is a clear indicator that more intentional focus on security awareness training is needed. Cognition will likely improve as government employees become more aware of the "big picture" need for good cybersecurity habits, and the positive and negative impacts their behavior can have on national security.



# Statistics for Government

Bar Plot: Score for All Dimensions in Government

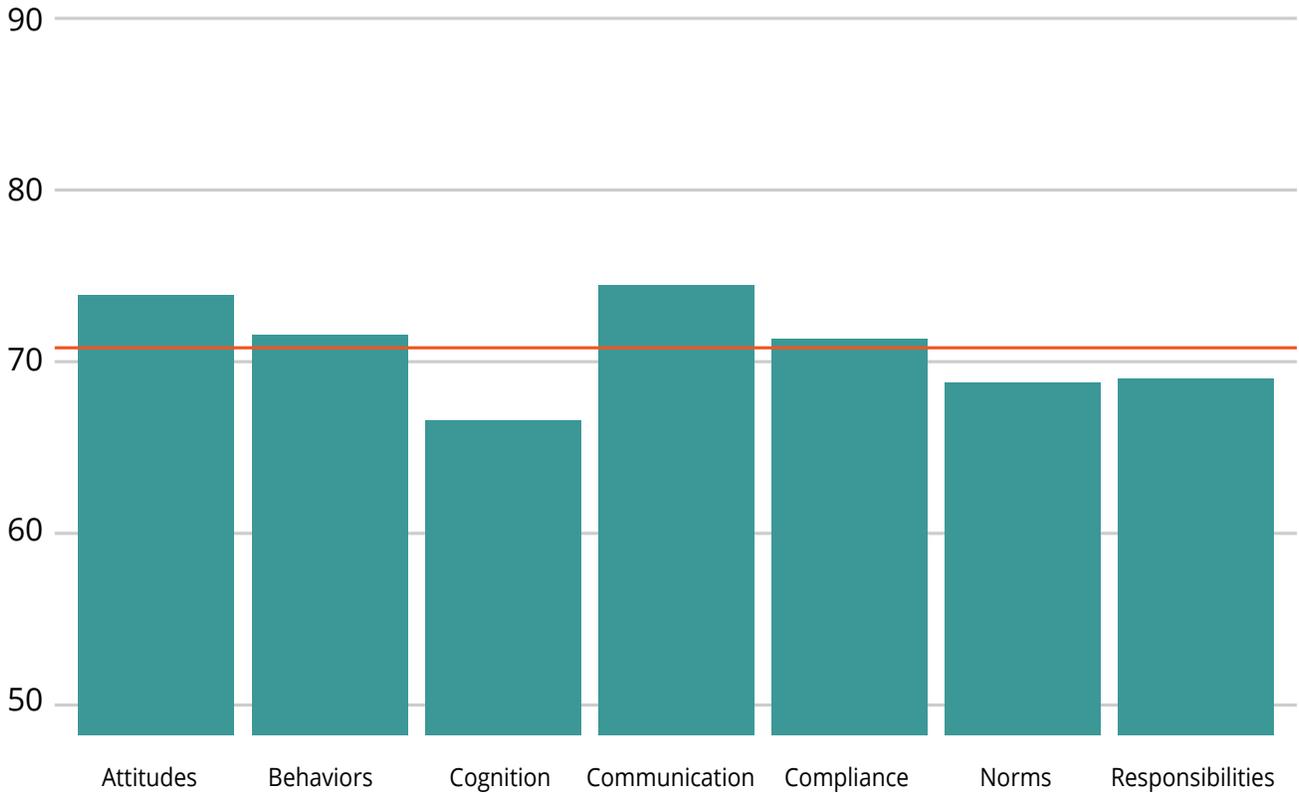


Table: Means per Dimension

Dimension	Mean	Dimension	Mean
Attitudes	74	Compliance	72
Behaviors	72	Norms	69
Cognition	67	Responsibilities	69
Communication	75	Security Culture Score	71

Box Plot: Security Culture Score for Government



Table: Total Number of Completed in Government

Industry	Number of Employees
Government	16,227

Table: Descriptive Statistics

Min	25%	Mean	Median	75%	Max
64	68	71	71	73	86

## Healthcare & Pharmaceuticals

The Healthcare and Pharmaceuticals sector has historically demonstrated a broad awareness of the need for security culture. This is due to a combination of regulatory requirements, adoption of best practices, and a sense of responsibility to “do no harm.”

The experience and understanding of risk management as a requirement for patient confidentiality fosters the need for an aggressive use of employee training. With a moderate security culture score of 74, organizations in this sector are often hardest hit by phishing attacks, which result in costly ransomware incidents (Source: KnowBe4 Phishing by Industry Benchmark Report 2020). Healthcare has fallen victim to some of the highest profile ransomware attacks in recent years.

The Healthcare and Pharmaceuticals sector shows a strong, positive attitude toward security. With a moderate score of 78 in the Attitudes dimension, it is likely that employees in this sector feel positive toward making adjustments and adopting security practices. The Communication dimension is at 77, demonstrating that organizations in this sector have generally adopted effective means of disseminating relevant information to employees when necessary. The Healthcare and Pharmaceuticals sector is also strong on adherence to policies. With a Compliance score of 74, employees are well informed of the policies and follow them quite well. This is reflected in the security behaviors of the employees. The Behaviors dimension looks at the security-related actions and hygiene of employees, and this dimension rates at a moderate 75.

### Areas for Improvement

The Healthcare and Pharmaceuticals sector demonstrates some room for improvement on the Norms dimension with a score of 72. 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 is vital in the growth of any risk management and training program. Scores of 71 in the Responsibilities dimension and 70 in the Cognition dimension indicate areas of potential improvement. The sector’s overall moderate score shows that the industry’s employees are willing to continually improve in their security culture.



# Statistics for Healthcare & Pharmaceuticals

Bar Plot: Score for All Dimensions in Healthcare & Pharmaceuticals

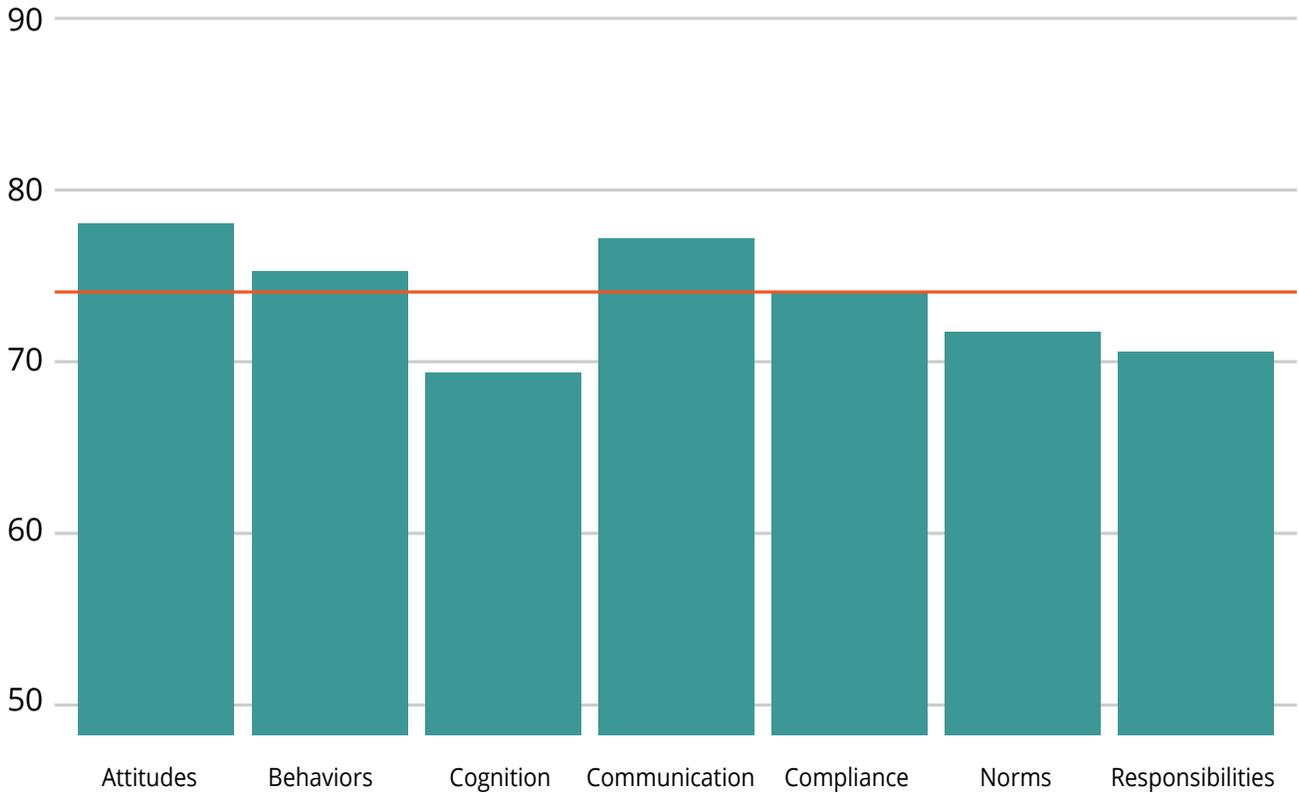


Table: Means per Dimension

Dimension	Mean	Dimension	Mean
Attitudes	78	Compliance	74
Behaviors	75	Norms	72
Cognition	70	Responsibilities	71
Communication	77	Security Culture Score	74

Box Plot: Security Culture Score for Healthcare & Pharmaceuticals



Table: Total Number of Completed in Healthcare & Pharmaceuticals

Industry	Number of Employees
Healthcare & Pharmaceuticals	9,114

Table: Descriptive Statistics

Min	25%	Mean	Median	75%	Max
67	70	74	74	77	84

## Insurance

The Insurance sector is a tremendous target for cyber criminals due to the significant amount of personal, financial, and medical information they hold. This is coupled with significant regulatory fines if they do not adhere to or fall behind on their respective security protocols.

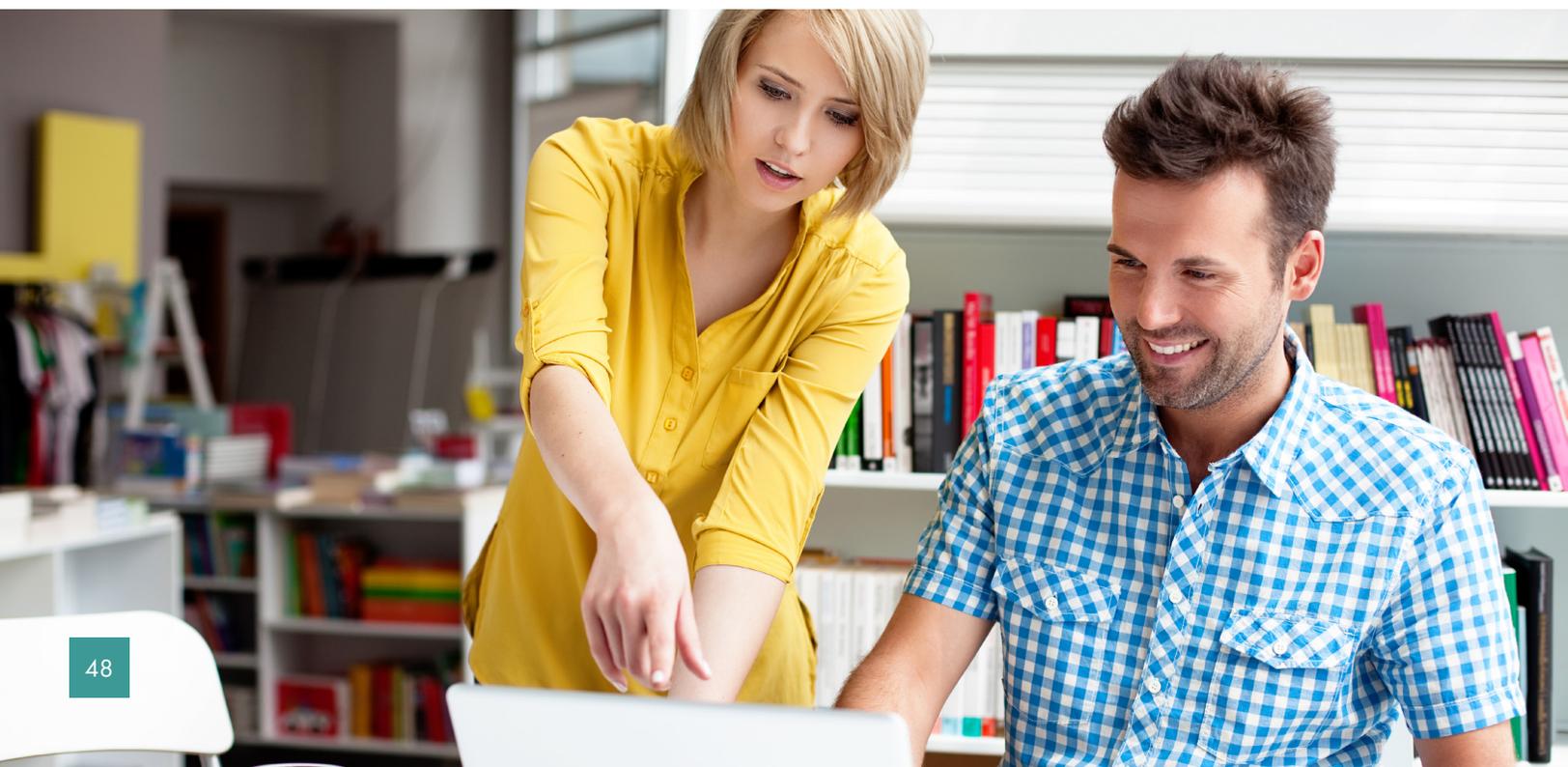
The Insurance sector showed moderate attitudes toward Communication, which scored 79. The need for strong, clear internal and external communications is paramount. Employees need to have timely information to respond to policy holders. They need to be able to convey a level of trust and confidence that keeps business intact. It is a clear strength for most in this industry.

With a score of 78 in the dimension of Attitudes, we see that employees within the Insurance sector have moderate feelings and beliefs related to the importance of their roles in security protocols and issues. To build strong security cultures, organizations within the Insurance sector should continue to reinforce favorable employee behaviors and empower them by enabling them with strong tools and processes.

### Areas for Improvement

The Insurance sector earned low-moderate performance in the dimensions of Cognition and Norms, both scored 71. 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 front line, to third-party partners. 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 unaccepted.



# Statistics for Insurance

Bar Plot: Score for All Dimensions in Insurance

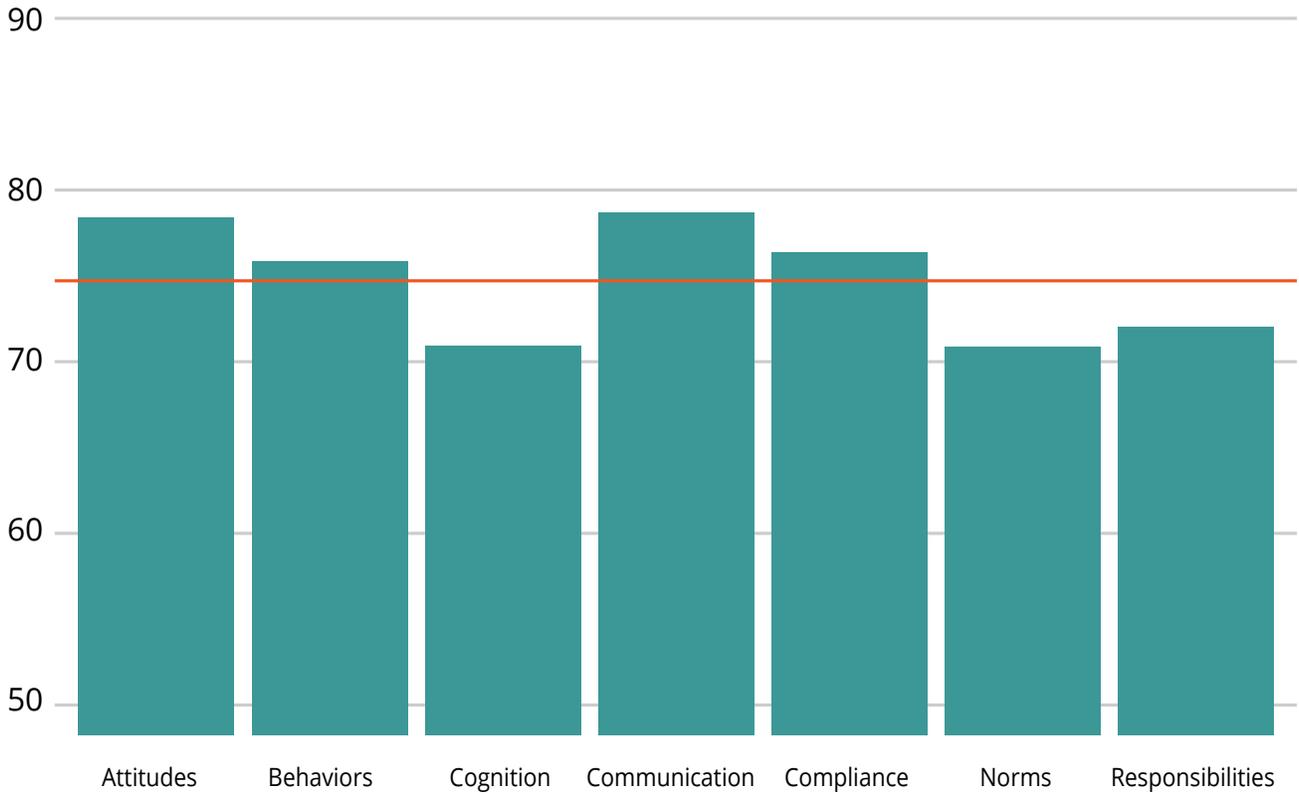


Table: Means per Dimension

Dimension	Mean	Dimension	Mean
Attitudes	78	Compliance	77
Behaviors	76	Norms	71
Cognition	71	Responsibilities	72
Communication	79	Security Culture Score	75

Box Plot: Security Culture Score for Insurance



Table: Total Number of Completed in Insurance

Industry	Number of Employees
Insurance	8,644

Table: Descriptive Statistics

Min	25%	Mean	Median	75%	Max
70	73	75	74	77	86

## Legal

As Legal firms understand, cybercrime will continue to surge in their sector due to the lucrativeness of the data that they hold and have access to. Confidential client documents including intellectual property, corporate/client finances, and evidence in matters of litigation, should they get in the hands of cyber criminals, could cause devastation. Proactively addressing security technology and knowledge gaps will be the true differentiator in this sector's ability to prevent breaches and to properly safeguard client data.

Legal firms are positive toward the Communication (76) and Attitudes dimensions (74), both scoring moderate overall. Legal firms show that being able to positively influence their employee thoughts and values will favorably impact the necessary attitudes to ensure that employees are always keeping security top of mind.

### Areas for Improvement

Like some healthcare establishments, Legal firms have long struggled with compliance to security awareness training. The moderate score in the dimension of Cognition (69) shows that at all levels required, continuous, engaging, and relevant security themed content is critical.

With the Norms dimension scoring 67, it is clear that more focus needs to be placed on how the unwritten security rules are being adopted and operationalized with employees at all levels, as role modeling starts at the top with partner compliance. Since there is a direct correlation between Behaviors and Norms, Legal firms should place a concerted emphasis on reinforcing norms to drive desired behaviors. "The task of building a security culture is thus to stimulate development of norms that support organizational security and ensure these norms become internalized. This way, adhering to a norm is intrinsically motivated and satisfying, and an individual will behave in line with norms even when there is no immediate social pressure or sanctions" (Source: The 7 Dimensions of Security Culture).



# Statistics for Legal

Bar Plot: Score for All Dimensions in Legal

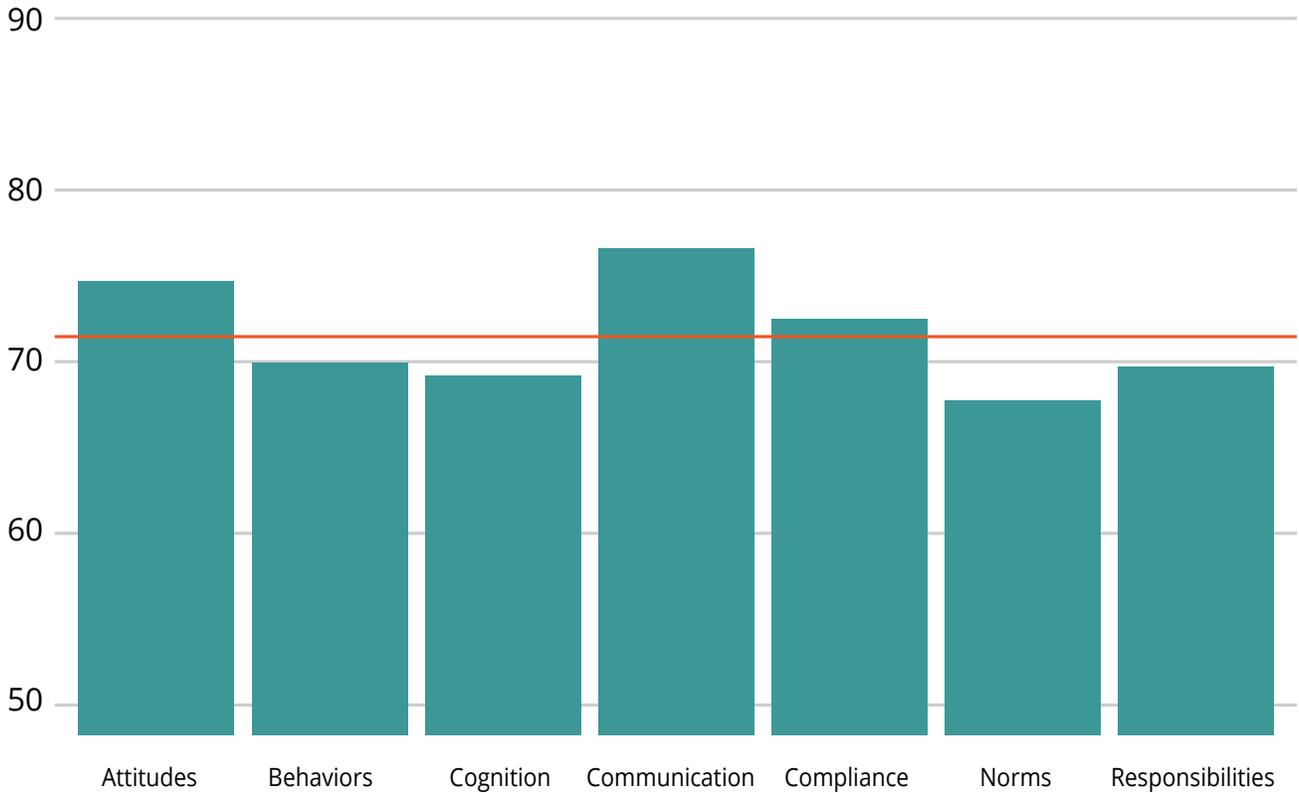


Table: Means per Dimension

Dimension	Mean	Dimension	Mean
Attitudes	74	Compliance	72
Behaviors	70	Norms	67
Cognition	69	Responsibilities	69
Communication	76	Security Culture Score	71

Box Plot: Security Culture Score for Legal

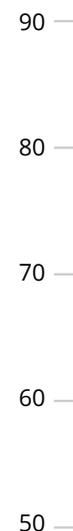


Table: Total Number of Completed in Legal

Industry	Number of Employees
Legal	750

Table: Descriptive Statistics

Min	25%	Mean	Median	75%	Max
66	69	71	72	73	77

# Manufacturing

The Manufacturing sector continues their journey toward digital transformation for supply chain, globalization, and increased connectivity of manufacturing platforms. The ongoing threat of intellectual property theft by cyber criminals or malicious insiders demands a greater security culture that is both persistent and relevant to stakeholders. The rapidly evolving landscape of 21st century Manufacturing from older, closer environments to interconnected internet-based infrastructure is lagging in a few dimensions, as seen by the Manufacturing sector's moderate security culture score of 71.

The Manufacturing sector indicates a positive attitude toward security. With a moderate score of 75 in the Attitudes dimension, it appears employees in this sector are positive toward adopting security practices to maintain pace with their industry's rapid evolution. This is also the case with the Communication dimension (76). The Manufacturing sector is moderate on their adherence to policies. With a Compliance score of 70, employees indicate areas of improvement regarding industry compliance. The Behaviors dimension looks at how employees behave regarding security, and this dimension rates at 72.

## Areas for Improvement

This sector showed moderate performance on the Norms dimension with a score of 69. This dimension measures the unwritten rules and how they are being adopted by the employees. A score of 67 in the Cognition dimension is a clear indicator that the Manufacturing sector has not kept pace with risk and threat awareness.

The Manufacturing sector is one of the most besieged and vulnerable to phishing attacks, (Source: KnowBe4 Phishing by Industry Benchmark Report 2020) and as such, improvement in both Norms and Cognition via improved training and education programs will better defend against ongoing cyber threats.



# Statistics for Manufacturing

Bar Plot: Score for All Dimensions in Manufacturing

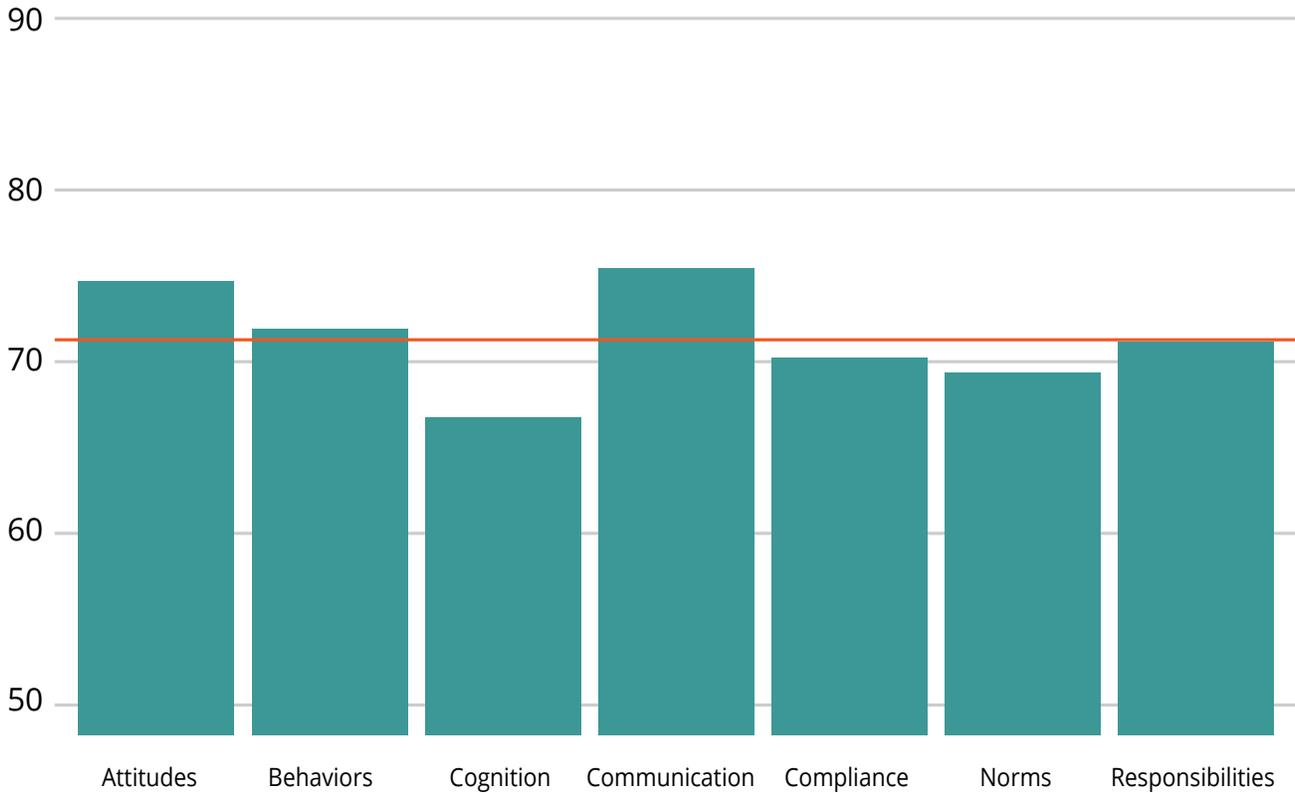


Table: Means per Dimension

Dimension	Mean	Dimension	Mean
Attitudes	75	Compliance	70
Behaviors	72	Norms	69
Cognition	67	Responsibilities	71
Communication	76	Security Culture Score	71

Box Plot: Security Culture Score for Manufacturing

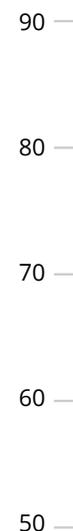


Table: Total Number of Completed in Manufacturing

Industry	Number of Employees
Manufacturing	10,308

Table: Descriptive Statistics

Min	25%	Mean	Median	75%	Max
59	69	71	71	74	79

## Not for Profit

Cyber criminals have long targeted Not for Profit organizations, knowing that they have very lean operating budgets and can sometimes justify only very little investment back into operations. As a result, cybersecurity is often neglected. Many Not for Profits exist on the fringe of what's considered a small business and do not believe they are big enough or important or relevant enough to give a criminal the kind of payday they are looking for. 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.

Not for Profits scored best in the dimension of Communication (78), 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 the overall security culture will help Not for Profits provide assurance to donors that their information and contributions are safe and used for only the intended purposes, thereby increasing long-term trust and confidence.

### Areas for Improvement

Most of the dimensions for Not for Profits fell in the moderate scoring range, with Cognition (69) and Norms (70) 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.



# Statistics for Not for Profit

Bar Plot: Score for All Dimensions in Manufacturing

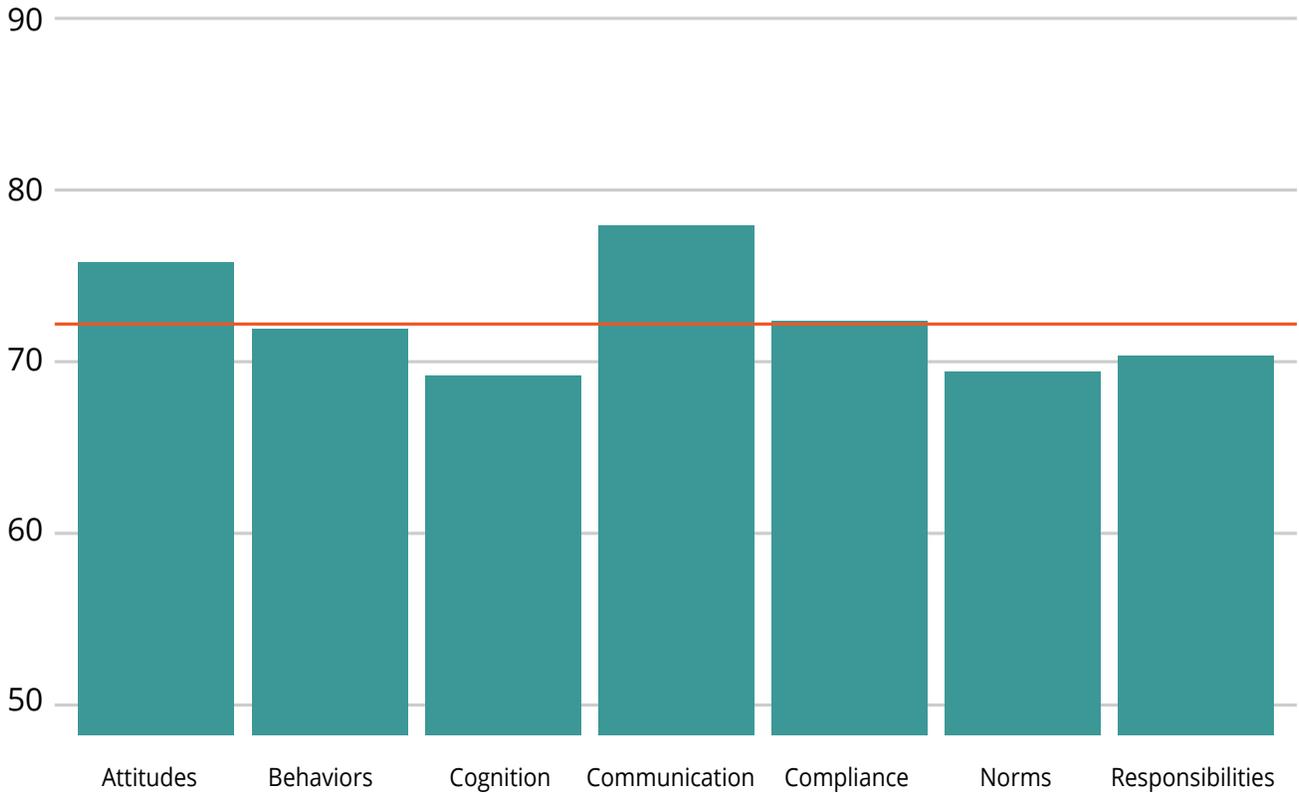


Table: Means per Dimension

Dimension	Mean	Dimension	Mean
Attitudes	76	Compliance	72
Behaviors	72	Norms	70
Cognition	69	Responsibilities	70
Communication	78	Security Culture Score	72

Box Plot: Security Culture Score for Not for Profit

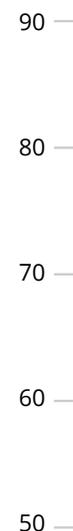


Table: Total Number of Completed in Not for Profit

Industry	Number of Employees
Not for Profit	2,808

Table: Descriptive Statistics

Min	25%	Mean	Median	75%	Max
63	70	72	72	75	84

## Other

The other sector represents industries that did not fit into the named industry sectors, or in which the data available in a named industry sector was less than 10 organizations.

Across this grouping, Communication scored moderate with a 76, while Attitudes also scored in the moderate range with a score of 75. 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 moderate scores in Cognition (68) and in Norms (69). 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.



## Statistics for Other

Bar Plot: Score for All Dimensions in Other

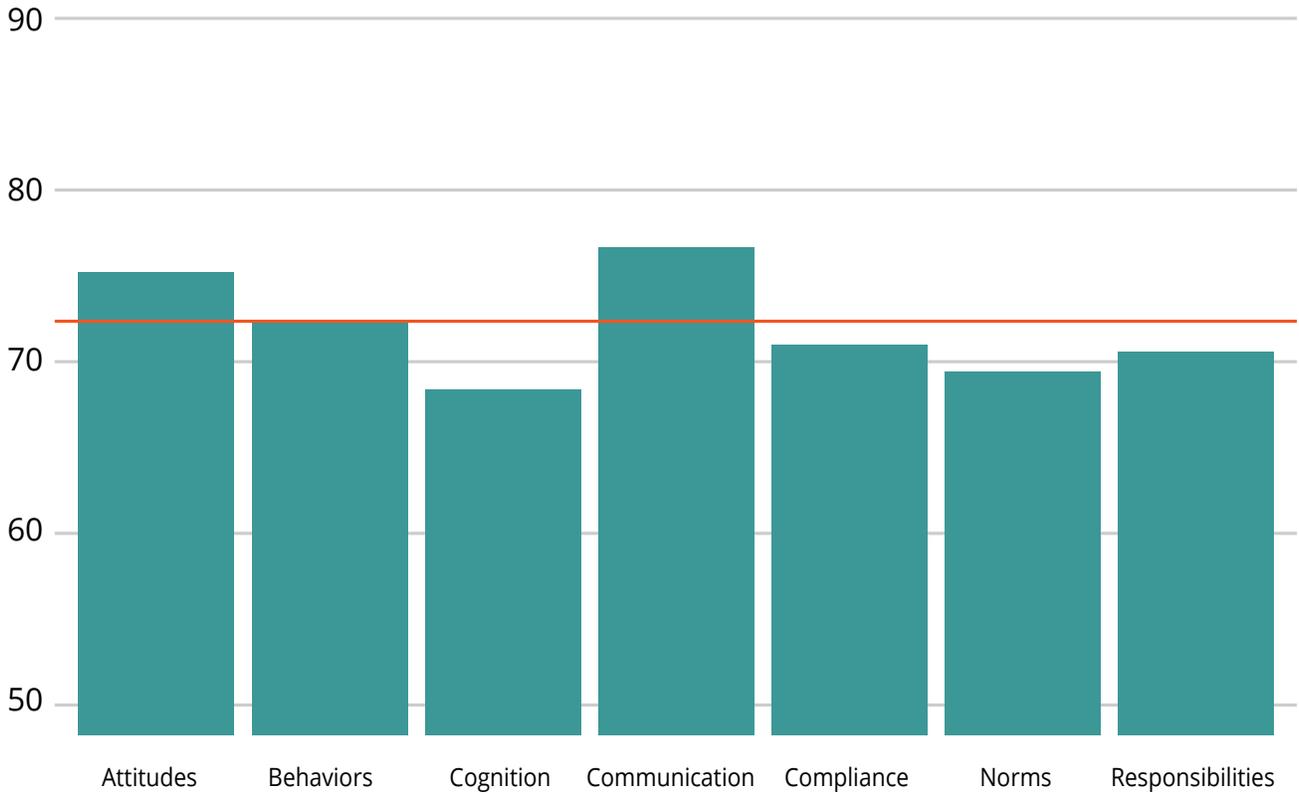


Table: Means per Dimension

Dimension	Mean	Dimension	Mean
Attitudes	75	Compliance	71
Behaviors	72	Norms	69
Cognition	68	Responsibilities	70
Communication	76	Security Culture Score	72

Box Plot: Security Culture Score for Other



Table: Total Number of Completed in Other

Industry	Number of Employees
Other	10,163

Table: Descriptive Statistics

Min	25%	Mean	Median	75%	Max
50	70	72	72	74	82

## Retail & Wholesale

The Retail and Wholesale sector has experienced several high-profile breaches in recent years and has subsequently directed more resources toward improving security culture. The challenge is, as always, finding a balance between fulfilling the needs of customers while increasing their overall security posture. This is reflected in the retail and wholesale sector's overall moderate security culture score of 71.

The Retail and Wholesale sector indicates a positive attitude toward security. With a moderate score of 75 in the Attitudes dimension, it is likely that employees in this sector are positive toward making adjustments and adopting security best practices. Further, we see that communication is the strongest aspect of Retail and Wholesale's security culture, with a Communication dimension at 76. A Compliance score of 71 indicates that employees are generally informed of relevant policies and follow them quite well. Slightly higher is the Behaviors dimension, which considers how employees behave regarding security. This dimension rates at 72.

### Areas for Improvement

The Retail and Wholesale sector has opportunities for improvement on the Norms dimension with a score of 69. This dimension is measuring the unwritten rules and how employees are adopting them. The Cognition dimension is another area where the Retail and Wholesale sector can improve. With a score of 67, 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.



# Statistics for Retail & Wholesale

Bar Plot: Score for All Dimensions in Retail & Wholesale

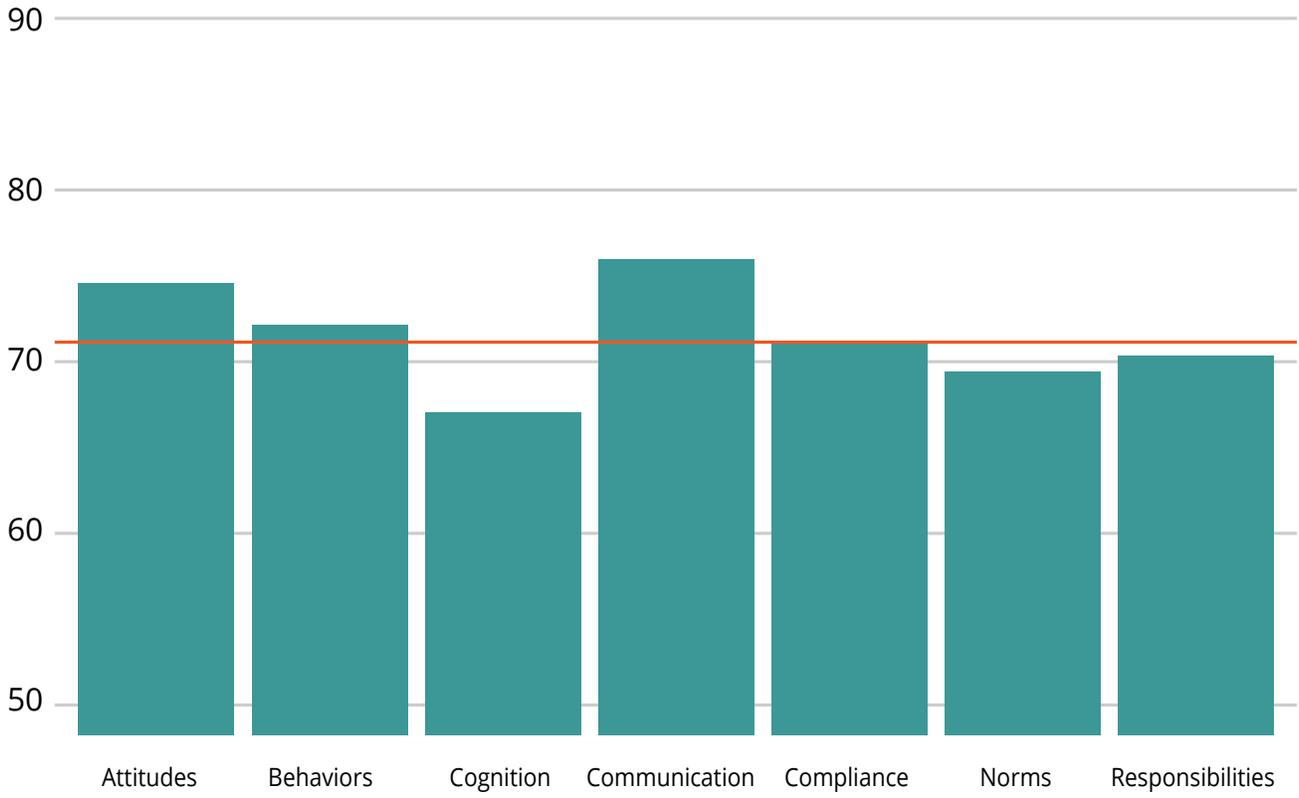


Table: Means per Dimension

Dimension	Mean	Dimension	Mean
Attitudes	75	Compliance	71
Behaviors	72	Norms	69
Cognition	67	Responsibilities	70
Communication	76	Security Culture Score	71

Box Plot: Security Culture Score for Retail & Wholesale



Table: Total Number of Completed in Retail & Wholesale

Industry	Number of Employees
Retail & Wholesale	5,171

Table: Descriptive Statistics

Min	25%	Mean	Median	75%	Max
62	70	71	71	73	82

# Technology

The Technology sector is in the business of managing security-related risk, though it often almost exclusively focuses on hardware and software-specific counter measures. End-user security behaviors, however, are not always equally accounted for. This is reflected in the Technology sector's moderate security culture score of 75.

The Technology sector does show positive attitudes toward security. With a score of 78 in the Attitudes dimension, it is apparent that employees in this sector are supportive of and positive toward making adjustments and adopting security practices. The Communication dimension is at 78; as expected, there are likely multiple vectors of communication throughout this sector that enable employees to access the data they need, when they need it. The Technology sector ranks as moderate regarding adherence to policies. There is positive performance indicated by the security behaviors of the employees. The Behaviors dimension looks at how employees behave regarding security, and this dimension rates at 75 points. Of note, the Technology sector has been one of the most targeted by phishing attacks (Source: KnowBe4 Phishing Industry Benchmark Report 2020), indicating the ongoing need to fine tune users' behaviors to guard against the threat of social engineering.

## Areas for Improvement

The Technology sector's areas for improvement are still rated as moderate on the security culture scale, with a score in the Norms dimension of 73. This dimension measures how well employees are adopting the unwritten security-related rules within an organization. Employee familiarity with policies and adherence to behavioral expectations are critical to a successful risk management program.

With a Compliance score of 73, employees should be provided additional awareness training related to policies and expectations to match the sector's strong scores in other dimensions. The Cognition dimension is another area where the Technology sector can improve. With another score of 73 in the Cognition dimension, it becomes clear that improved efforts in awareness training is likely the gateway to unlocking improvement in the Compliance and Norms dimensions.



# Statistics for Technology

Bar Plot: Score for All Dimensions in Technology

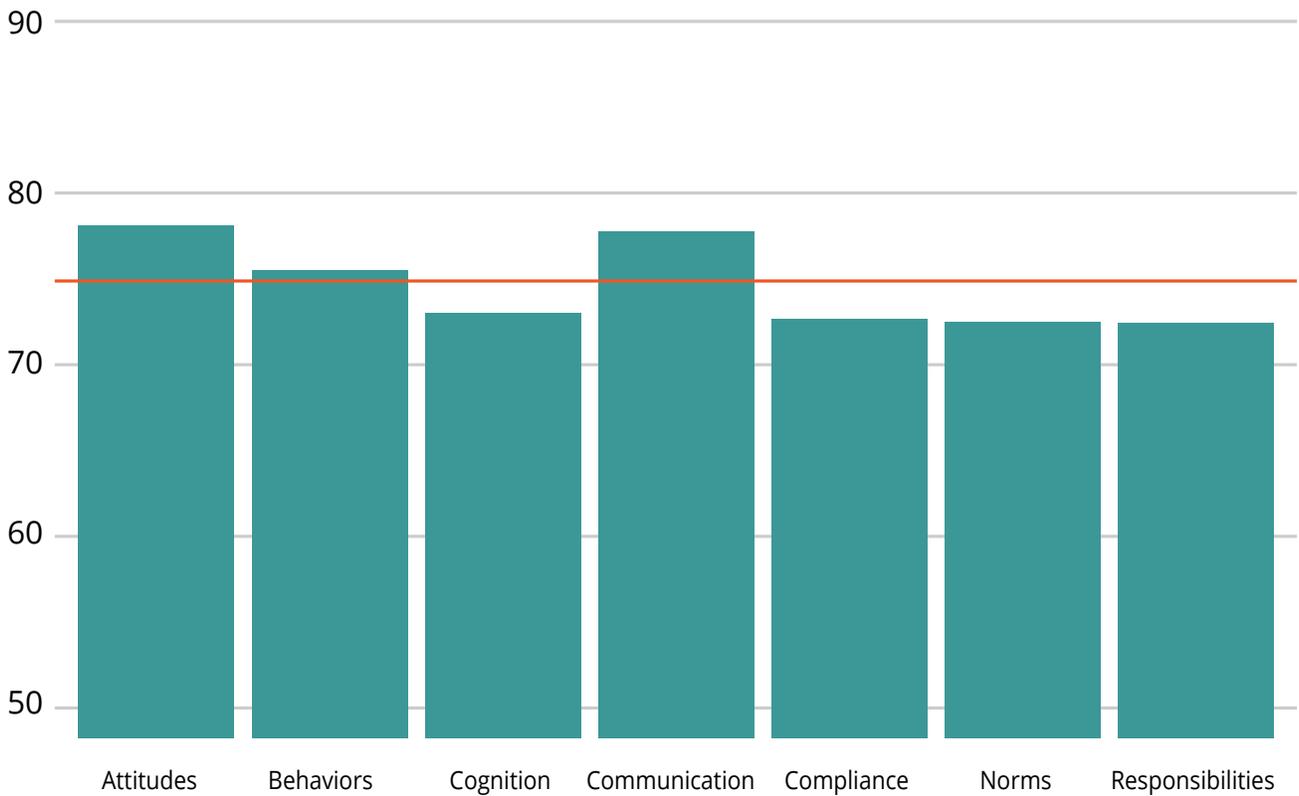


Table: Means per Dimension

Dimension	Mean	Dimension	Mean
Attitudes	78	Compliance	73
Behaviors	75	Norms	73
Cognition	73	Responsibilities	73
Communication	78	Security Culture Score	75

Box Plot: Security Culture Score for Technology



Table: Total Number of Completed in Technology

Industry	Number of Employees
Technology	13,865

Table: Descriptive Statistics

Min	25%	Mean	Median	75%	Max
56	72	75	75	77	85

# Transportation

As the Transportation sector embraces internet-connected, innovative new technologies to enter the next stage of digital transformation, they face cybersecurity challenges from the resulting broader cyber attack surface. Many areas within the Transportation sector were designed and implemented long before there was a concept of security culture. These challenges are reflected in their moderate security culture score of 70.

For a sector with only a low moderate security culture score, there are some encouraging points of strength when we get to the dimensional analysis. Attitudes (74) and Communication (75) were the highest rated dimensions for this sector. With a score of 74 in the Attitudes dimension, it is likely that employees are positive toward making adjustments and adopting security practices when requested. The Communication dimension score of 75 indicates that Transportation organizations are generally good at getting important information to employees effectively.

## Areas for Improvement

The Transportation sector can improve upon their adherence to policies. With a Compliance score of 70, employees can be made better aware of their industry's policies, and organizations should evaluate how they are currently encouraging and enforcing security-related activities. This score correlates with the security behaviors of the employees; and the Transportation sector scored a 71 in the Behaviors dimension.

Scores for the Transportation sector reveal the need for performance improvement on both the Norms and Responsibilities dimensions, each with a score of 68. The Norms dimension is measuring the unwritten rules and how employees are adopting them. Employee knowledge and competence is critical in any industry's understanding of security culture, and this is another area where the Transportation sector can improve. A score of 67 in the Cognition dimension is a clear indicator that there is a strong need for improved training and education programs. There is a strong connection between Responsibilities, Cognition, and Norms; and the Transportation sector should focus on all dimensions to elevate this sector's overall security culture.



# Statistics for Transportation

Bar Plot: Score for All Dimensions in Transportation

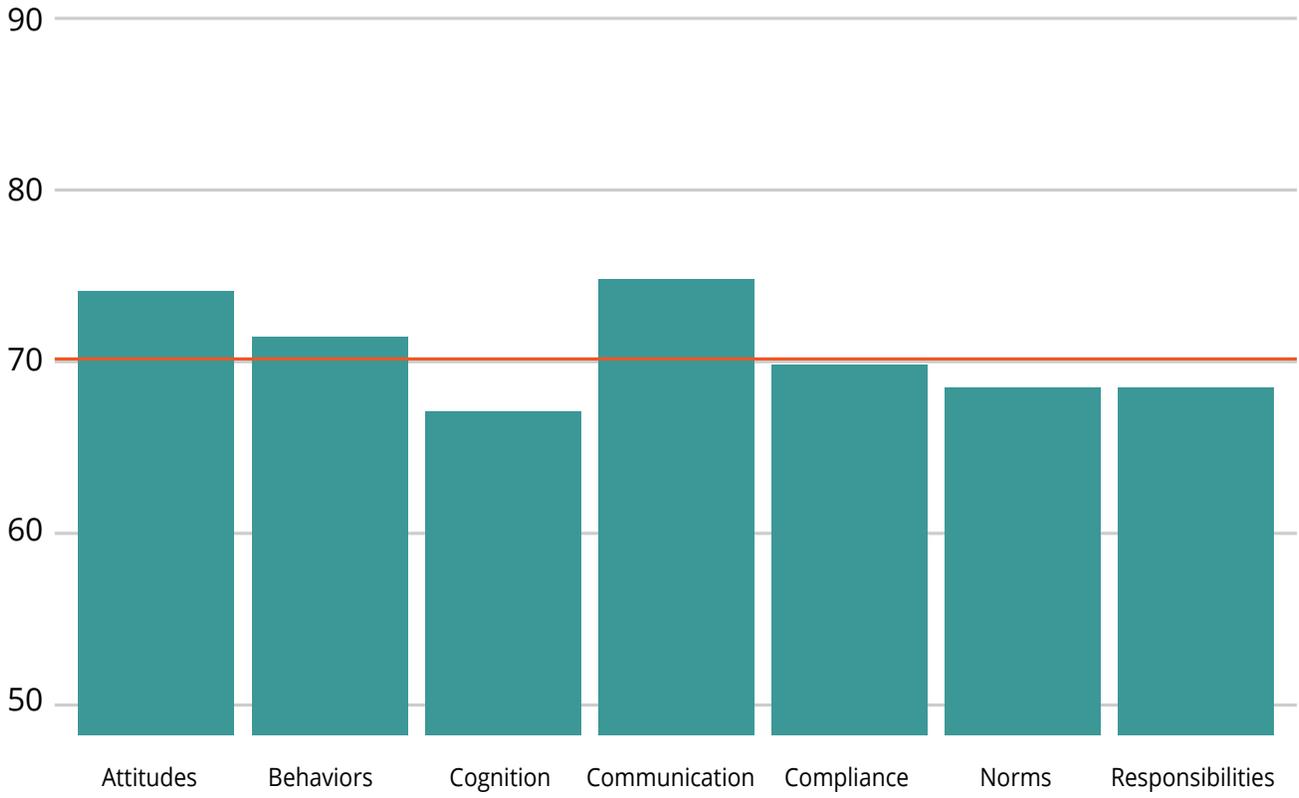


Table: Means per Dimension

Dimension	Mean	Dimension	Mean
Attitudes	74	Compliance	70
Behaviors	71	Norms	68
Cognition	67	Responsibilities	68
Communication	75	Security Culture Score	70

Box Plot: Security Culture Score for Transportation



Table: Total Number of Completed in Transportation

Industry	Number of Employees
Transportation	2,673

Table: Descriptive Statistics

Min	25%	Mean	Median	75%	Max
60	68	70	71	73	78

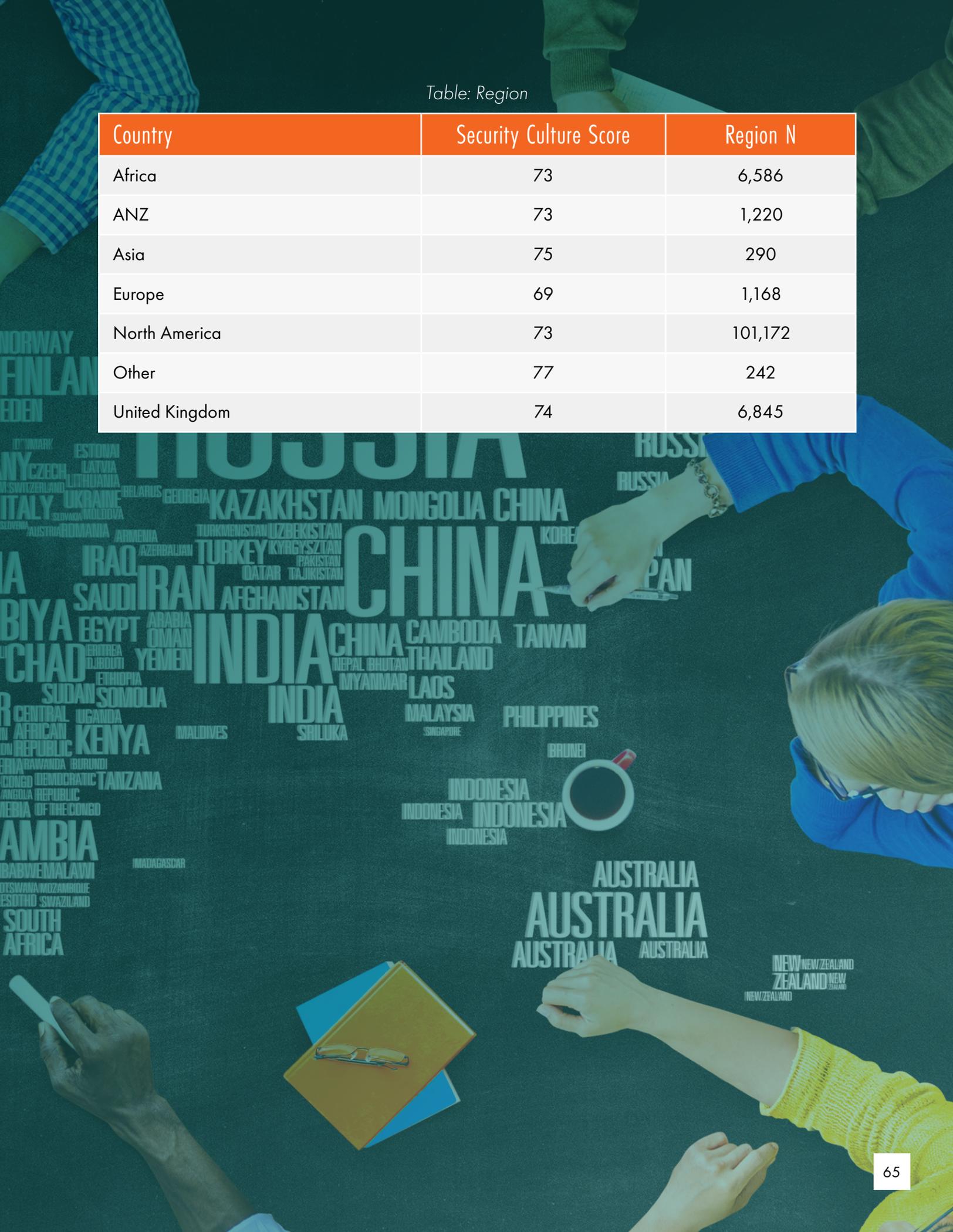
# Regional Data

Table: Country

Country	Security Culture Score	Country N
India	79	162
Mexico	79	164
Netherlands	75	209
United States	74	95,285
Australia	73	714
Bermuda	73	238
Kenya	73	357
New Zealand	73	506
United Kingdom	73	6,607
Canada	72	5,887
South Africa	72	6,096
Belgium	70	199
Switzerland	68	259
France	62	225
Norway	59	228

Table: Region

Country	Security Culture Score	Region N
Africa	73	6,586
ANZ	73	1,220
Asia	75	290
Europe	69	1,168
North America	73	101,172
Other	77	242
United Kingdom	74	6,845



# About the Report

This report was created by CLTRe, a research division of KnowBe4, using the highest academic standards. The report leverages anonymized data from KnowBe4's Security Culture Survey. The sample size represents 1,107 surveyed organizations around the world, with more than 120,000 employees across 17 industry sectors, effectively making this the largest report of its kind published to date.

## Methodology

### 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 based on a scientific approach that integrates survey methodology, statistics, and scientific findings from security culture research and psychometrics<sup>[12]</sup>. 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 March 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. Soon, CLTRe will offer responses with multiple time points. All data analysis was performed in the software environment R (r-project.org).

### Data Preprocessing

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. A listwise deletion of missing data was conducted. Furthermore, only organizations with more than 10 valid employee responses were included.

### Statistical Analyses

The values that employees provide on the 28 security culture items are transformed into eight metrics for each organization: security culture score and score for each dimension. All scores have a range from zero to 100. By aggregating scores to an organization rather than at the employee level, we ensured that the effects of organization size on industry benchmarks were neutralized. The unique algorithm for this transformation was designed by CLTRe and based on complex conceptual understanding of organizational security culture.

### Data Size

The data consists of 120,050 employees and 1,107 organizations. After data cleansing, the final sample consists of 119,312 employees and 954 organizations that completed the Security Culture Survey. Data was collected from more than 20 countries.

---

12 To Measure Security Culture, CLTRe, 2017: <https://get.clt.re/whitepaper-to-measure-security-culture-a-scientific-approach/>

Table: Number of Employees and Organizations With Complete Data per Industry

Industries	Organizations	Employees
Banking	90	10,873
Business Services	60	2,799
Construction	26	4,447
Consulting	35	1,429
Consumer Services	14	1,471
Education	38	4,940
Energy & Utilities	33	3,484
Financial Services	140	10,146
Government	73	16,227
Healthcare & Pharmaceuticals	65	9,114
Insurance	41	8,644
Legal	10	750
Manufacturing	66	10,308
Not for Profit	52	2,808
Other	72	10,163
Retail & Wholesale	40	5,171
Technology	88	13,865
Transportation	11	2,673
Total	954	119,312

Table: Employee Count per Country

Country	N of Employees
United States	95,285
United Kingdom	6,607
South Africa	6,096
Canada	5,887
Australia	714
New Zealand	506
Kenya	357
Switzerland	259
Bermuda	238
Norway	228
France	225
Netherlands	209
Belgium	199
Mexico	164
India	162
Botswana	88
Philippines	88
United Arab Emirates	78
Suriname	40
Finland	31
Namibia	28
Greece	17
Zimbabwe	17

# Authors

## 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, 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.



## Anita-Catrin Eriksen

Anita-Catrin Eriksen holds a Bachelor of Arts in Social Sciences and Humanities from University College Utrecht in the Netherlands. She also holds 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. Eriksen is the research assistant at CLTRe, a KnowBe4 company. As the research assistant, she analyses data and conducts and advises on best practices for research. She works to ensure that insights into security culture and behavioral information security come from reliable and valid data.





## 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 Women in Defense.



## 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).



*This report uses the highest academic standards to leverage anonymized data from 1,107 surveyed organizations around the world, with more than 120,000 employees across 17 industry sectors, effectively making this the largest report of its kind published to date.*

## 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. In 2017, Aimee Laycock joined the team to help commercialize the platform. As a research-first company, CLTRe published the first Security Culture Report in 2017, measuring 11,212 employees in Northern Europe, at the time the largest global study into the human factors that influence security. Working with the EU, ENISA, SINTEF, and the Norwegian Research Council, CLTRe provided the industry with important facts and figures.

CLTRe AS was acquired by KnowBe4, Inc in 2019, and is committed to bringing our 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 34,000 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.

