KnowBe4 Research

THE SECURITY CULTURE REPORT 2022

Global Trends in Security Culture

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

Table of Contents

Executive Summary

The 2022 Security Culture Report (SCR) is the largest, globally recognized research into security awareness, behavior and culture available. The SCR offers unique insights which allow organizational leaders to better understand how employees view security within their organizations. This information is also leveraged by business leaders to ensure necessary investment dollars are allocated to the most critical part of the security infrastructure: the human element.

The SCR provides a number of key resources essential in understanding and measuring an organization's security culture.

A Standard Way to Measure and Report

This report uses the globally recognized Security Culture Index. The use of a standard index offers direct value by allowing the reader to compare the information presented in a meaningful way.

The index ranges are as follows:

- 90 up to 100 Excellent
- 80 up to 89 Good
- 70 up to 79 Moderate
- 60 up to 69 Mediocre
- 0 up to 59 Poor

> ...Ensure necessary investment dollars are allocated to the most critical part of the security infrastructure: **the human element**.

To identify where on the index an organization belongs, the Security Culture Survey (SCS) is used. Leveraged by 2,910 companies worldwide, the SCS is the most comprehensive measurement instrument available to assess an organization's security culture.

The Global Pandemic Improved Security Culture

The impact of the global pandemic showed that while some industry sectors have reduced their security culture significantly, others have improved. The most significant finding is that no industry is found to have Poor or Mediocre security culture scores. Although all industry sectors have a security culture that is considered Moderate, many of the industries include organizations that have been rated as Good.

Security Culture Varies Around the World

Our results show that some regions and countries are reporting a much better security culture than others. A notable example is the United States of America, which generally trends higher on all aspects of security culture compared to other countries. Behind the USA is Europe, which has a much larger variation in security culture between countries, which results in a lower average. Africa, Asia and South America generally show a lower security culture, suggesting that more work is needed.

> The impact of the global pandemic showed that while some industry sectors have **reduced** their security culture significantly, others have **improved**.

Industry Benchmarking With Trends

In 2022, we have introduced new graphics to the industry benchmark to make it easier to review and process. The new trend graph places the current score into context. We also provide a breakdown based on organizational size, allowing you to more accurately assess where your organization sits. Additionally, each industry benchmark is presented on a single page, making it easy to print and share only the information you need.

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

Board Level Concern

Security culture has garnered attention from board-level executives. The SCR provides all levels of executives, management and practitioners with the necessary context and data to help navigate the complexity of security within their own organization. In the ever-increasing landscape of social engineering, and the challenge that the human factors bring to any organization today, it is critical that top-level management understand the risk and the impact that security awareness, behaviors and culture has.

Defining Security Culture

It is important to note that the phrase "security culture" is beginning to find its way into the lexicon of security leaders. CISOs and security executives now commonly cite security culture as being a critical element of their security posture. But there is a problem—security leaders have vastly different definitions of security culture, meaning that they do not really know what they are all in agreement about.

We define security culture as the ideas, customs and social behaviors that influence an organization's security. A common definition makes it possible to discuss the same thing, in the same way. We all know that if you do not measure something, that something does not exist.

Introduction

The SCR is produced annually by KnowBe4 Research, allowing us to analyze the security culture of thousands of organizations globally. It is the largest report ever published on this topic, with an increasing data set year-over-year. The report offers the reader insight into the state of security measures and their impact, through the human factor's lens. As such, this unique report offers important information to the global security industry and should be used by top management within an organization to inform their security program improvements for 2022.

The first SCR was published in 2017, by the Norwegian research company CLTRe. After being acquired by KnowBe4 in 2019, the research unit became KnowBe4 Research, and is considered the leading security culture research organization in the world.

In the 2022 report, we introduce several new sections. For the first time, we can present security culture trends, exploring how industries change over time. We also presented data that helped explain the impact of the pandemic, and that should be used to understand how your industry sector performs. Additionally, we have added a regional breakdown, where we offer two different views into security culture around the world: 1) general security culture; 2) the impact that organizational size has on security culture globally.

The Security Culture Industry Benchmark offers a deep dive into each industry sector. We have made several changes to this section in this report, introducing trends and organizational size perspectives.

The 2022 SCR is divided into the following sections:

- Introduction
- What Is Security Culture—Definition of: security culture, 7 dimensions of security culture and the Security Culture Index
- A Global Perspective of Security Culture—Security culture as seen around the world. This section includes information on security culture based on organizational size and across regions.
- Security Culture Industry Trends—The evolution of security culture over time
- Industry Benchmark—Detailed information about each industry sector
- Method—Shares data, tables and methodology
- About—Information about the authors and KnowBe4

This report is robust in offering a lot of industry relevant information that we are certain you will find value in.

Changes in the Security Culture Report 2022

The following new sections have been added to the 2022 report:

- *A Global Perspective on Security Culture*—Regional data breakdown of Europe, USA, Canada and Latin America with regional map visualizations. This section also includes security culture as measured by organizational size – security culture and dimension scores by size of organizations: small, medium and large.
- *Trends*—How different industries have performed regarding security culture over the past two to three years.

These new sections have one thing in common—the data is represented visually via graphs and maps. We believe visualizing the data makes the information easier to digest. However, if you prefer to see the actual numbers in table format, you can find this in the Methodology section.

To make space for all this new content, the Detailed Analysis of Security Culture section was removed. Our plans are to publish this type of analysis in a different report in the future. Additionally, the Comparing Dimensions Scores Across Industries section has been discontinued with the data now available on each industry page.

Another change this year is the Industry Benchmark section. This year, the boxplots have been removed to allow space for trend data on all dimensions and an analysis of scores by organizational size. We are excited about this change, as it allows for a more detailed and long-term perspective on security culture. For those still interested in the statistics associated with the boxplot, you can find these in the Methodology section.

Lastly, there have been some changes to the industries included in this year's report.

- Internet and Software Services, which was previously in the Other category, is now in Technology.
- Hospitality, also in the Other category, is now an independent benchmark.
- SCS data where the industry is unknown has been removed and therefore has eliminated the Other category.

Our continuous content review and subsequent changes allow us to keep providing you with the most relevant and useful data available.

Join the Discussion

We appreciate that you are taking the time to read this report. If you enjoy what you read and want to join the discussion, please share the report and your comments online, using your preferred platform.

Please reference the report as the 'Security Culture Report 2022 by KnowBe4 Research'. We also ask that if you want to give people a copy of the report, that you provide them with the link, rather than the PDF.

If you have any press inquiries, please reach out to our PR team at pr@knowbe4.com.

Security Culture—A High-Level Perspective

In this section, we offer a brief overview of what security culture is.

What Is Security Culture

We define security culture as: The ideas, customs and social behaviors that influence an organization's security.

This definition makes it clear that security culture is a combination of thought processes and knowledge, the habits that employees have adapted and the behaviors that are demonstrated when in the workplace. By workplace, we mean any such place where employees perform their work. We define security broadly.

With this definition in mind, organizations should focus their efforts on a combination of employee engagement with assessments and training, improve process and procedures and by implementing technology that makes it easy for the employee to do the right thing.

For more in-depth information on what security culture is, and how to successfully implement a security culture program at your organization, refer to *The Security Culture Playbook, An Executive Guide To Reducing Risk and Developing Your Human Defense Layer* by Perry Carpenter and Kai Roer (Wiley, 2022).

Security Culture Dimensions

We systematically evaluate culture across seven distinct dimensions:

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

Security Culture Index

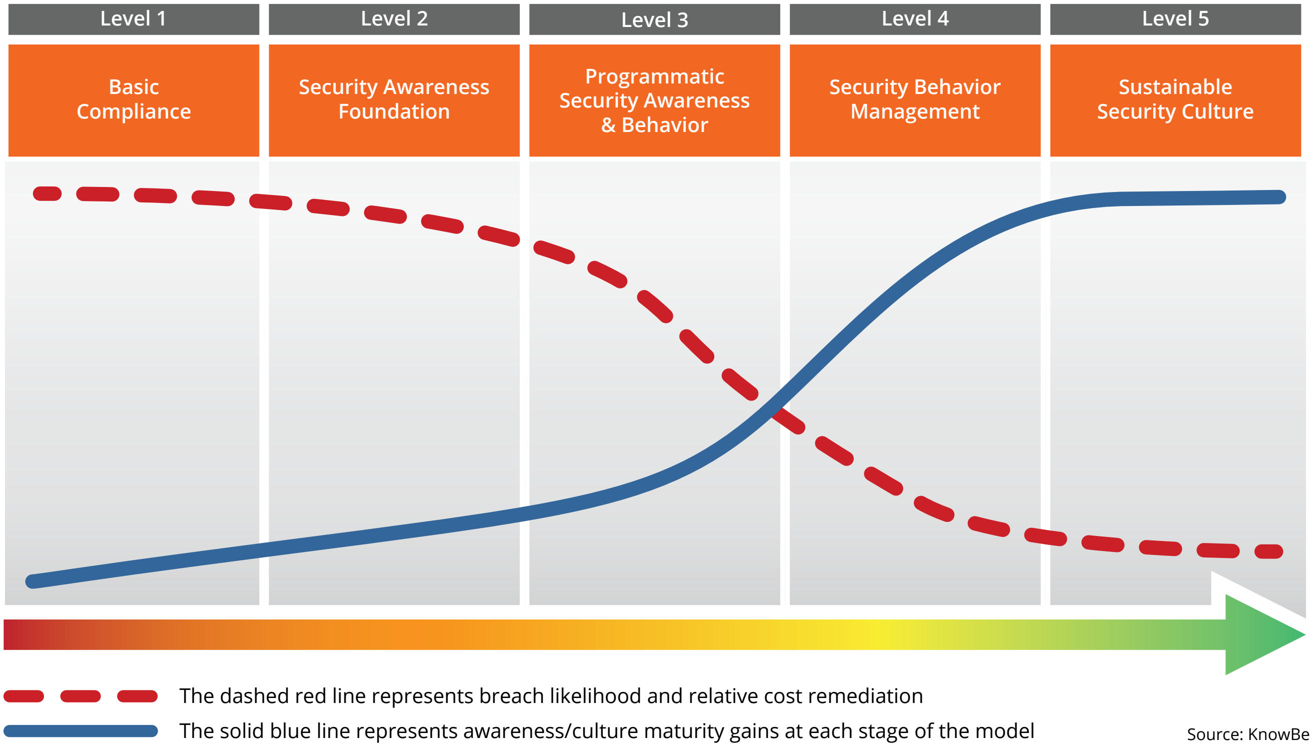
The Security Culture Index (SCI) is the global index for rating organizations based on their security culture score. The index was created by the team of researchers at KnowBe4 Research and is calculated by analyzing the security culture of thousands of organizations around the world. More details on the index itself, and the direct risk attached to each level, can be found in the research paper Security Culture and Credential Sharing, available for download at: https://get.clt.re/credential-sharing-research/

- 90 up to 100 Excellent
- 80 up to 89 Good
- 70 up to 79 Moderate
- 60 up to 69 Mediocre
- 0 up to 59 Poor

Note: *None of the industry sectors have demonstrated Excellent or Good security culture this year.*

The Security Culture Maturity Model

The data-driven and evidence-based Security Culture Maturity Model, developed by KnowBe4 Research, is the industry's first maturity model specifically geared to measure security culture. The model is fueled by KnowBe4's massive security awareness, behavior and culture dataset.


Level 1
Basic Compliance
Level 2
Security Awareness Foundation
Level 3
Programmatic Security Awareness & Behavior
Level 4
Security Behavior Management
Level 5
Sustainable Security Culture
- - - The dashed red line represents breach likelihood and relative cost remediation
━━ The solid blue line represents awareness/culture maturity gains at each stage of the model

Source: KnowBe4

Figure 1: Security Culture Maturity Model.

The Five Maturity Levels

The model's range accounts for organizations with no formal or intentional awareness, behavior or culture plan other than to achieve basic compliance (Level 1) all the way up to the most sophisticated organizations that seek to push beyond the pack and are actively working to shape even the unwritten rules and social dynamics of how their employees value security. Learn more about these levels below.

Level 1	Basic Compliance	Bare minimum of training Limited metrics "Check the box"
Level 2	Security Awareness Foundation	At least annual and onboarding training Occasional phishing simulations Focus on variety of content
Level 3	Programmatic Security Awareness & Behavior	Intentional awareness program with integrated tools Quarterly training with simulated phishing Focus on security-aware behaviors
Level 4	Security Behavior Management	Continuous training across varied delivery methods and audiences Heavy use of integrated tools to inform training strategy Program focused on real behavior change
Level 5	Sustainable Security Culture	Program that intentionally measures, shapes and reinforces security culture Multiple methods of behavior-based encouragement Security values woven through fabric of entire organization

You can learn more about the Security Culture Maturity Model in the white paper available for download here: https://www.knowbe4.com/security-culture-maturity-model

A Global Perspective on Security Culture

Measuring security culture is a global concern. Understanding the security culture of your workplace is proving increasingly important for the security posture of the organization. As we demonstrated in the 2021 SCR, 9/10 global security leaders believe that security culture is a critical factor to their successful implementation of a security program. The gap between the acceptance of security culture being critical and the implementation of a security culture program, is demonstrated by the lack of data from many countries. Of particular interest, outside Europe and North America, we have noted a dramatic drop in organizations measuring security culture, leaving them blindsided when it comes to assessing the human factors of security.

Below, we share regional breakdowns for your reference, but the important message is that organizations must step up their game and invest in security awareness, behavior and culture in the years to come. This is not a nice to have, it is a critical asset used to reduce risk and improve security.

Security culture is found in every organization, all around the world. In this section, we are comparing security culture and commenting on the observations and measurements. When looking at security culture from a satellite perspective, the variation between regions is small, with only two points between the worst performing and the best performing.

Global Overview

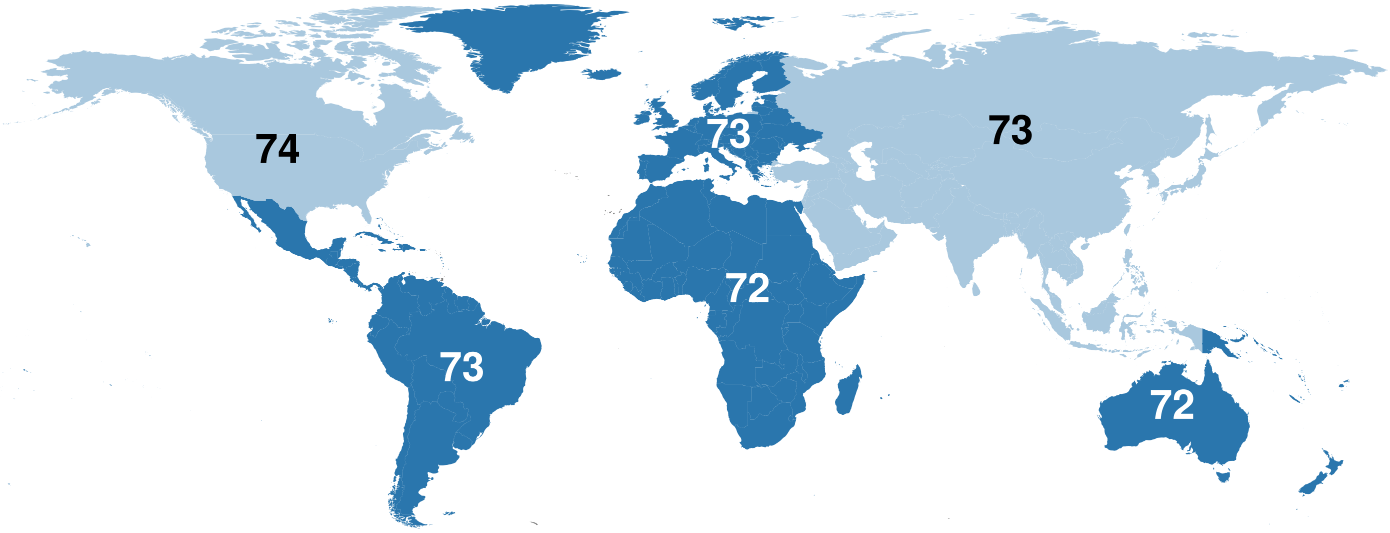


Figure 2: The global perspective of security culture.

North America scored 74 (the best), with the rest of the world comparable to Europe and Asia scoring 73, and Latin America, Africa and Oceania scoring 72.

This global overview easily gives a false understanding—that all regions perform similarly and that things are not too bad. But the reality is more nuanced, and shocking, than what the aggregated picture may indicate. That becomes clear as we dig into each of the regions.

In the breakdown below, we use the same scale across all regions and countries, to make it easy to visually compare regions and countries.

Sample sizes are not large enough to further break down the regions of Central and South America, Africa and Asia. These regions are lagging behind in security investments in general, and especially in security awareness, behavior and culture. In 2022, it is common knowledge that human factors have a dramatic impact on security, regardless of the geographical location of an organization. It is therefore our strong recommendation that organizations and nations around the world invest in programs and strategies to dramatically improve the assessment and training of employees.

Security Culture According To Organizational Size Worldwide

In this section, we examine security culture based on organizational size:

- **Large**–1,000+ employees and are represented with the red line.
- **Medium**–250 to 1,000 employees and are shown with the green line.
- **Small**–less than 250 employees and are represented with the blue line.

We first show a global overview, before breaking it down into regions.

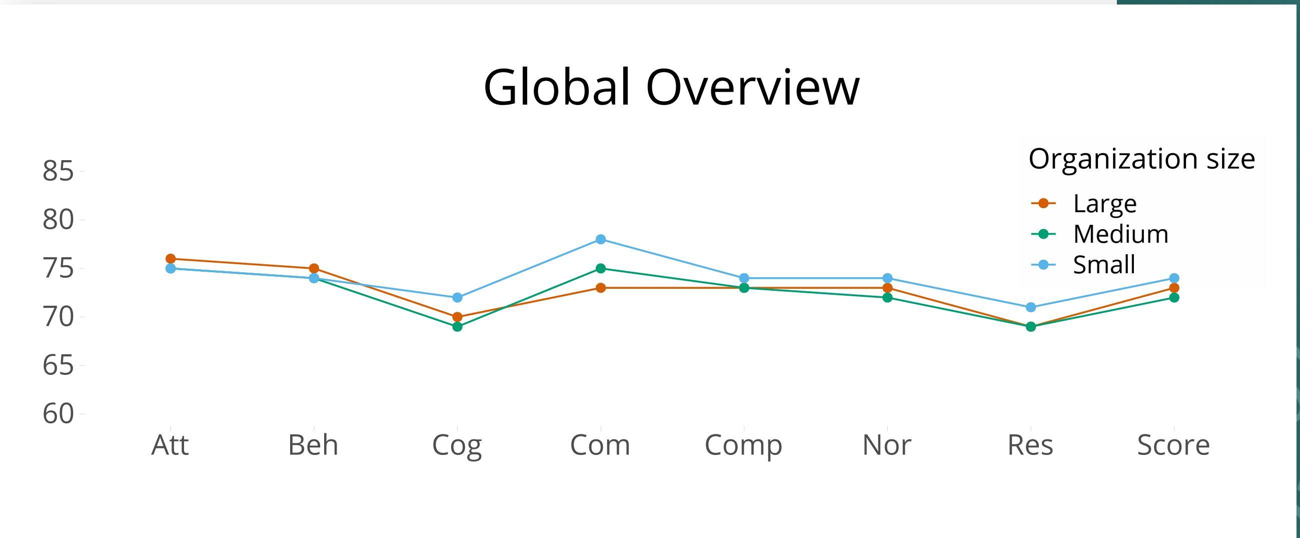


Figure 3: Security culture as seen by organizational size (Global overview).

We see an interesting pattern emerge when examining the security culture scores globally. At first glance, it seems like security culture is similar regardless of the size of the organization. In addition, the two valleys in the graph are appearing in the same place: in the Cognition and the Responsibility dimensions.

Upon closer inspection, we see that large organizations report better attitudes and behaviors than smaller organizations. This may be related to the fact that many larger organizations are likely to be publicly traded, and thus regulated. On the other hand, small organizations scored better on all other dimensions, something that is really visible on the Communication dimension, where the Large organizations scored five points less. Communication tends to be easier in smaller groups, and this is clearly demonstrated here.

Security Culture in Africa

In Africa, there is a tradition and interest in security culture, especially in South Africa (73), where we expected a higher level of security culture than was achieved. In the other countries in Africa where we have data, we see very wide variations in security culture, which is likely explained by limited sample sizes. We expect to see more African countries measuring security culture in the future. In the meantime, we urge organizations and governments to focus on the human aspects of security and invest in education and training.

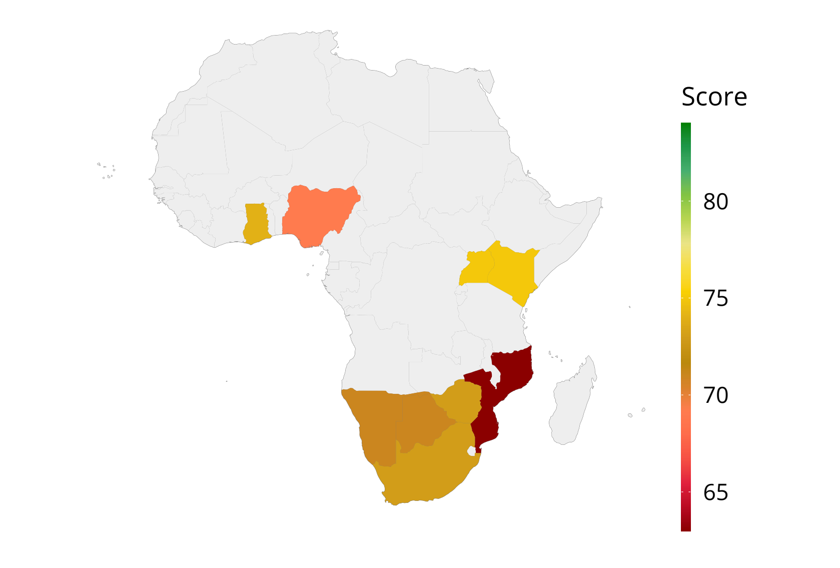


Figure 4: Security culture score in Africa. The sample size varies from country to country. For more details, please refer to the method section.

Security Culture in Africa According to Organizational Size

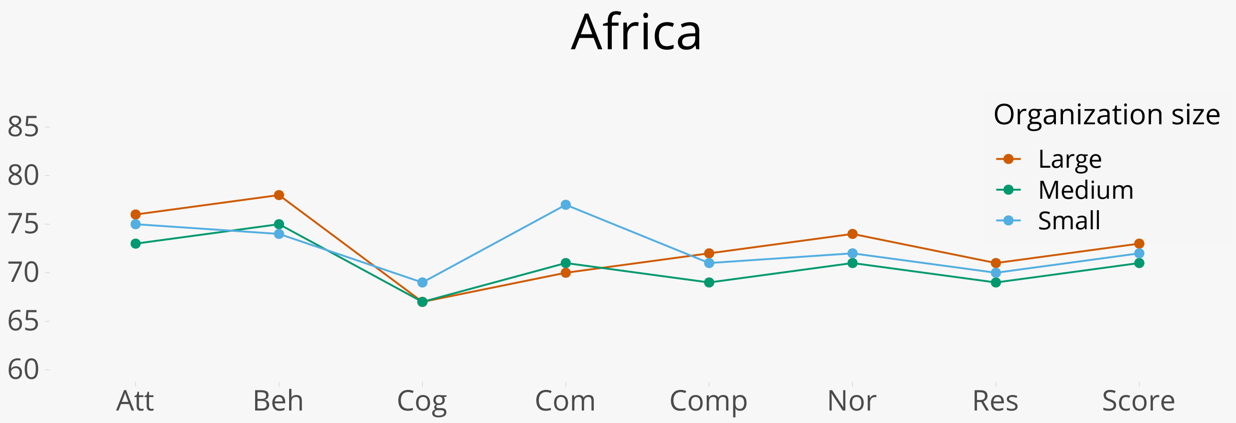


Figure 5: Security culture in Africa as seen by organizational size.

In Africa, we see that Large organizations generally do better than others when it comes to security culture. There are two notable differences: the Cognition and Communication dimensions, where Small organizations perform much better than the others. Africa has a sample size of 52 organizations and 14,121 employees.

Security Culture in Asia

In Asia, we see a wide variation of security culture scores across nations. While Japan (76) is doing reasonably well, countries like Malaysia (66) and Indonesia (67) show an alarmingly low security culture index score. Our general recommendation for organizations in Asia is to invest in security awareness, behavior and culture programs.

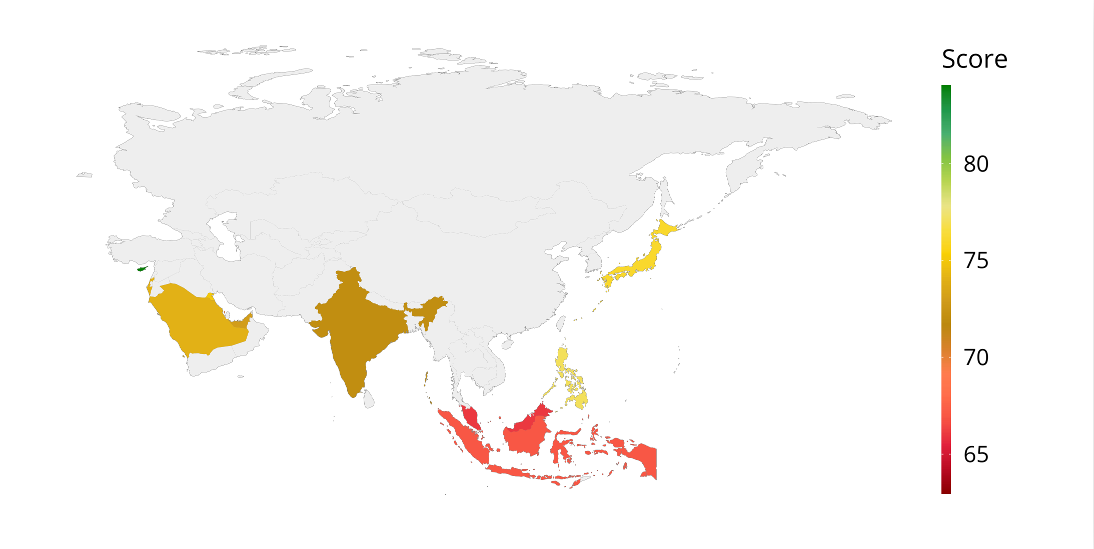


Figure 6: Security culture score in Asia. The sample size varies from country to country. For more details, please refer to the method section.

Security Culture in Asia According to Organizational Size

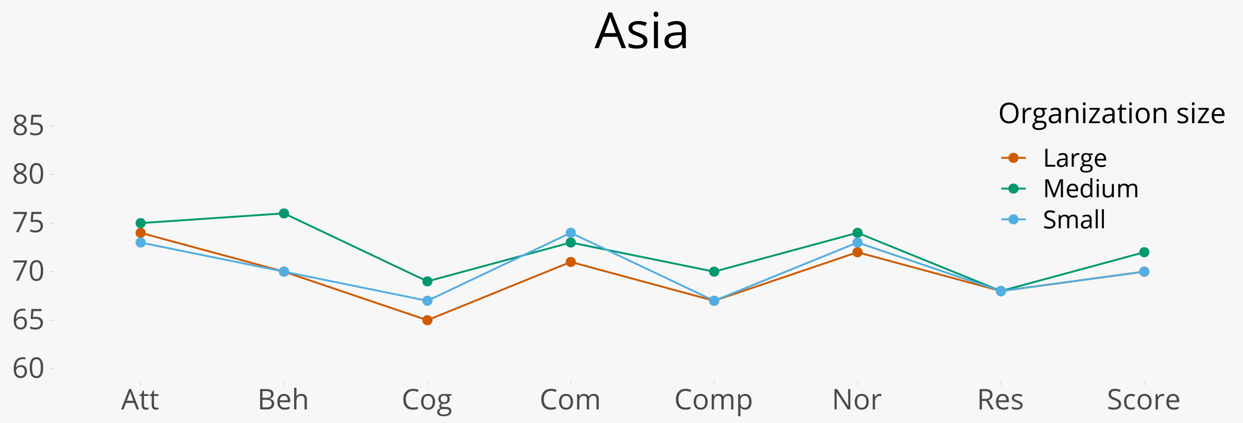


Figure 7: Security culture in Asia as seen by organizational size.

In Asia, we see that organizational size is a smaller factor than in some other regions. With the exception of Medium organizations on the Attitudes and Behaviors dimensions, we see that the organizational size has little impact on security culture. Our findings may be skewed due to the comparably small sample size of 39 organizations and 15,095 employees across the continent.

Security Culture in Europe

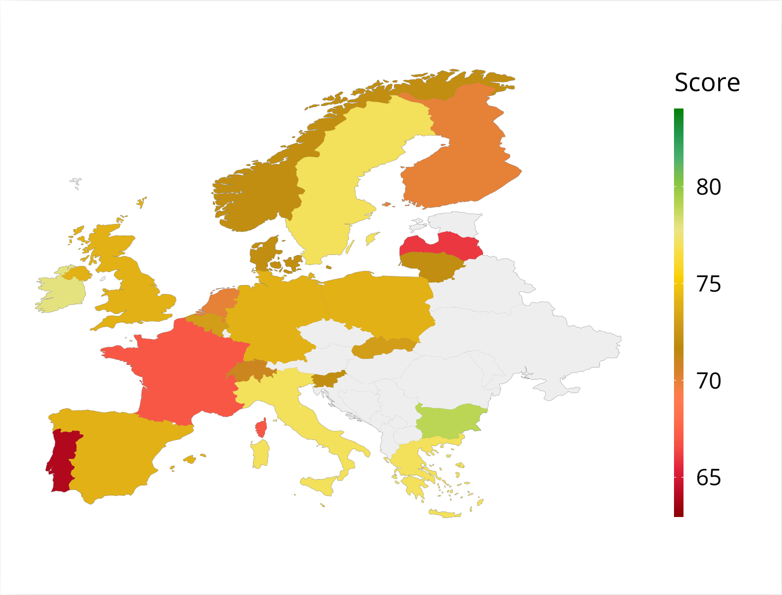


Figure 8: Security culture score in Europe. The sample size varies from country to country. For more details, please refer to the method section.

In Europe (73), we observe large variations in security culture between countries. The worst performing countries are Portugal (64), Latvia (66) and France (67). These results may be due to small sample sizes in these countries, suggesting that security measures in general are lacking. We urge these countries to implement measures to improve their security and reduce risk.

On the more favorable end of the spectrum, we find Sweden (77) and Ireland (78), both often being considered technologically advanced. Along with them, we also find that Italy (77) and Bulgaria (79) score higher. Even so, no countries in Europe report a Good score on the Security Culture Index. Considering the ongoing geopolitical situation, our recommendations are that countries in Europe take action to improve their security culture by assessing their employees and implementing training and education programs to ensure the right security behaviors.

Security Culture in Europe According to Organizational Size

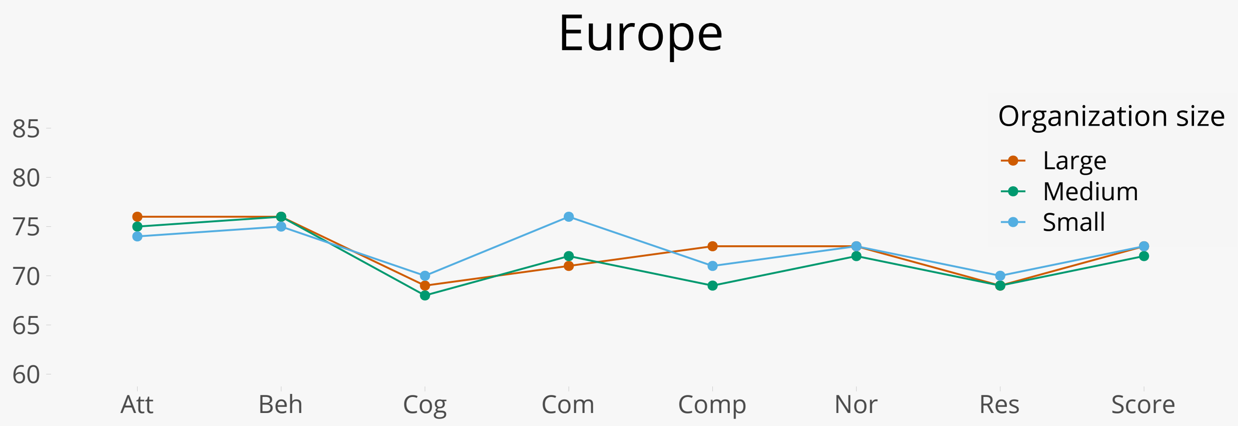


Figure 9: Security culture in Europe as seen by organizational size.

Europe shows a relatively consistent variation across the size of organizations. The most notable difference is seen in the dimensions Communication and Compliance. Small organizations are dramatically better at communicating than other organizations. Large organizations score the highest when it comes to compliance. Europe has a sample size of 141 organizations and 30,016 employees.

Security Culture in North America

The North American region in this report consists of the USA and Canada. As a region, North America is more favorable than the rest of the world, with an average score of 74. When looking at the region from a national perspective, we see that the region is showing differences in the security culture scores. Below, we break down the results according to state levels for the USA and Canada.

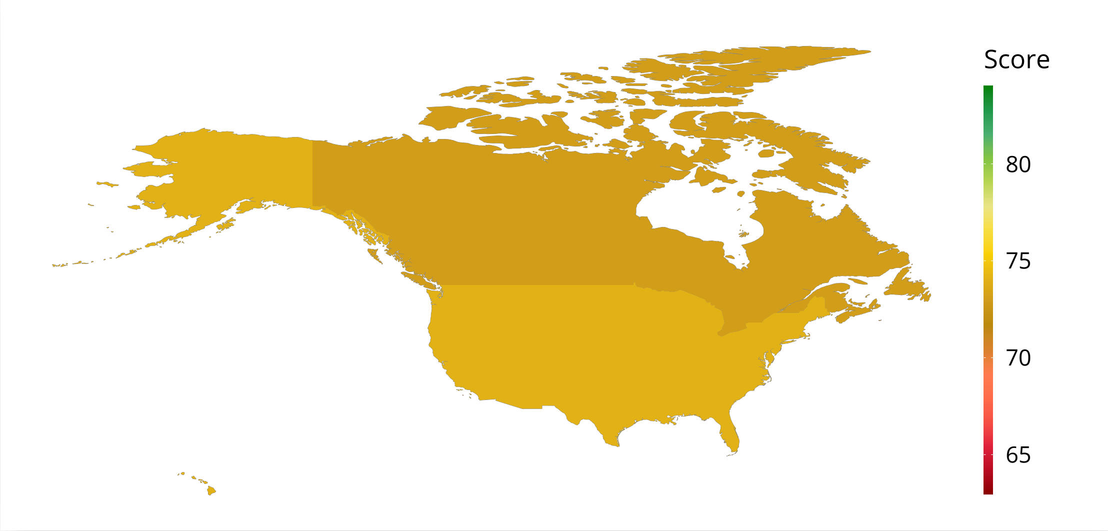


Figure 10: Security culture score in North America. The sample size varies from country to country. For more details, please refer to the method section.

Security Culture in North America According to Organizational Size

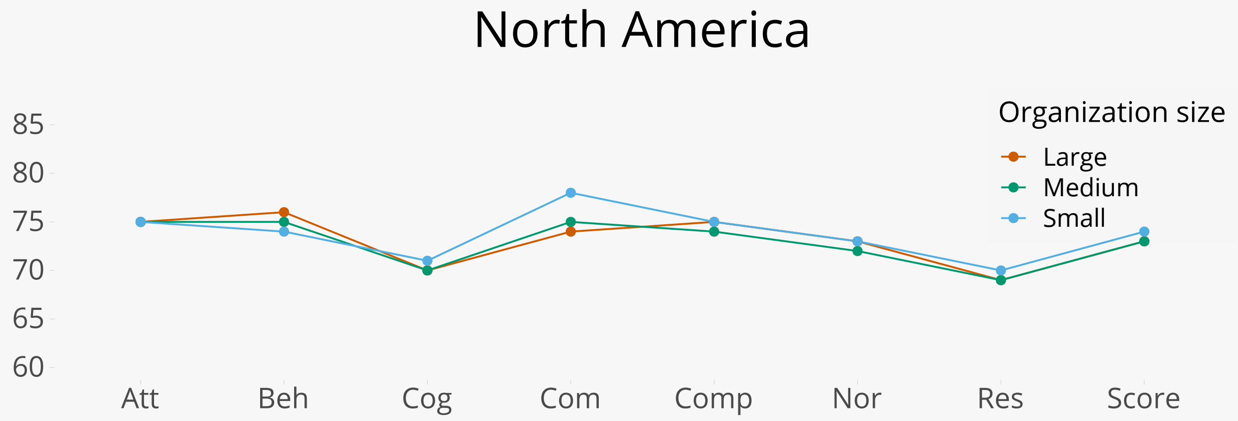


Figure 11: Security culture in North America as seen by organizational size.

Security culture in North America reflects small differences based on organizational size. The most notable differences are in the dimension of Communication, where Small organizations outperform the others. The other dimension that stands out is Behavior, where Large organizations perform better and Small organizations underperform. It is also worth noting that the North American and European security cultures follow a very similar pattern. The sample size for all of North America is 1,144 organizations and 184,701 employees.

Security Culture in Canada

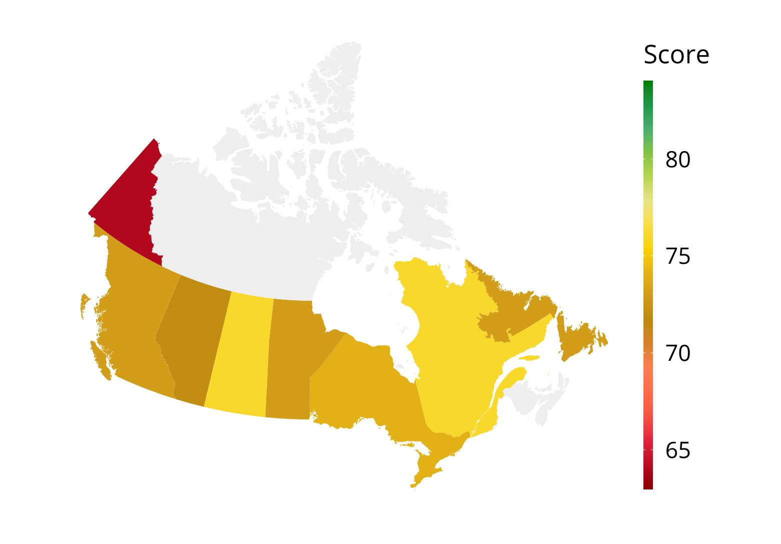


Figure 12: Security culture in Canada. The sample size varies from country to country. For more details, please refer to the method section.

Canada had a large variation between the state scores, ranging from the best performing Quebec (76) and Saskatchewan (76) to the worst performing Yukon (64). A score of 64 is ranked as Mediocre on the Security Culture Index and signifies a large increase in human factor risks compared to the level above, Moderate.

Sample sizes in many Canadian states are low, suggesting that most organizations do not have even a minimum level of security measures in place. It is our recommendation that organizations in these regions implement adequate security culture measures, including training and assessments.

Security Culture in Canada According to Organizational Size

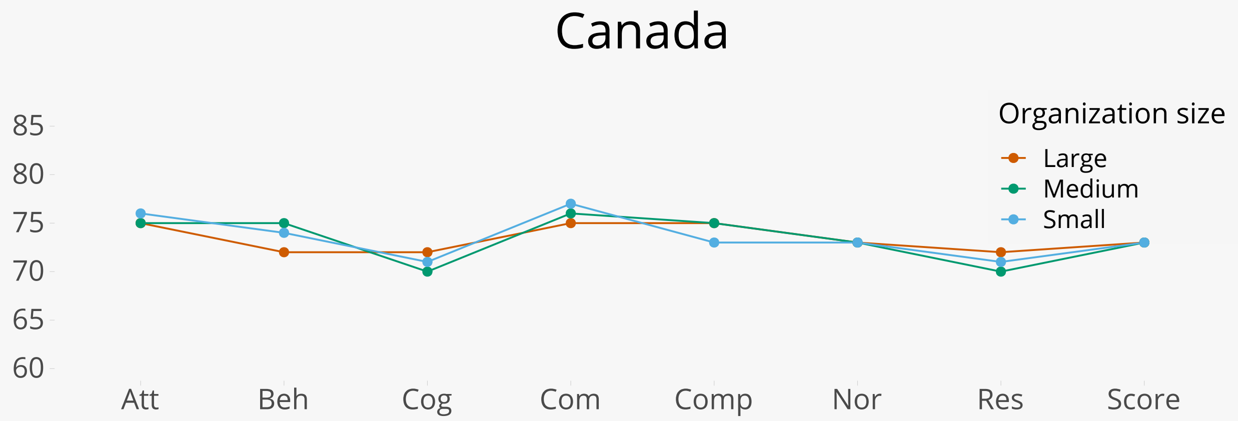


Figure 13: Security culture in Canada as seen by organizational size.

In Canada, we see the overall security culture score of all three sizes of organizations (73) is consistent. Canada also shows very little variation in the dimension scores across the size of organizations. Overall, the best performing dimensions are Attitudes and Communication, in which Small organizations outperform the others. Looking closer, Small and Medium sized organizations appear to perform the same or better than Large organizations on every dimension except Compliance and Responsibility. However, performance of these two dimensions is relatively low for all organizations in Canada. Canada has a sample size of 76 organizations and 7,108 employees.

Security Culture in the United States of America

The USA is underperforming when it comes to security culture. When breaking the country into the states, a more detailed image emerges: the national score is hiding differences in the scores between the states. We observe that both East and West coast states are generally performing with better scores, with Vermont (77) and Rhode Island (77) on the East coast and Oregon (77) on the West coast performing more favorably than the rest.

Inland states like South Dakota (72), Iowa (72) and Arkansas (72) are examples of states that perform poorly.

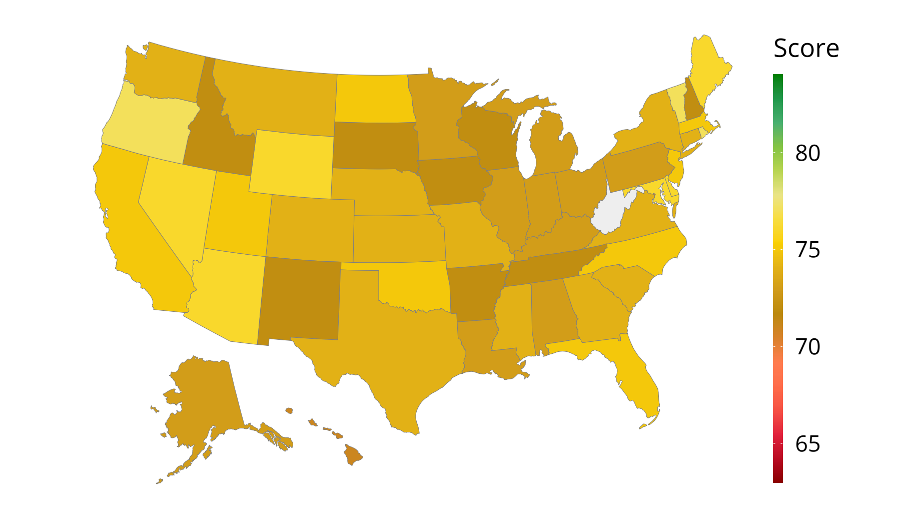


Figure 14: Security culture in the United States of America. The sample size varies from state to state. For more details, please refer to the method section.

Security Culture in the United States of America According to Organizational Size

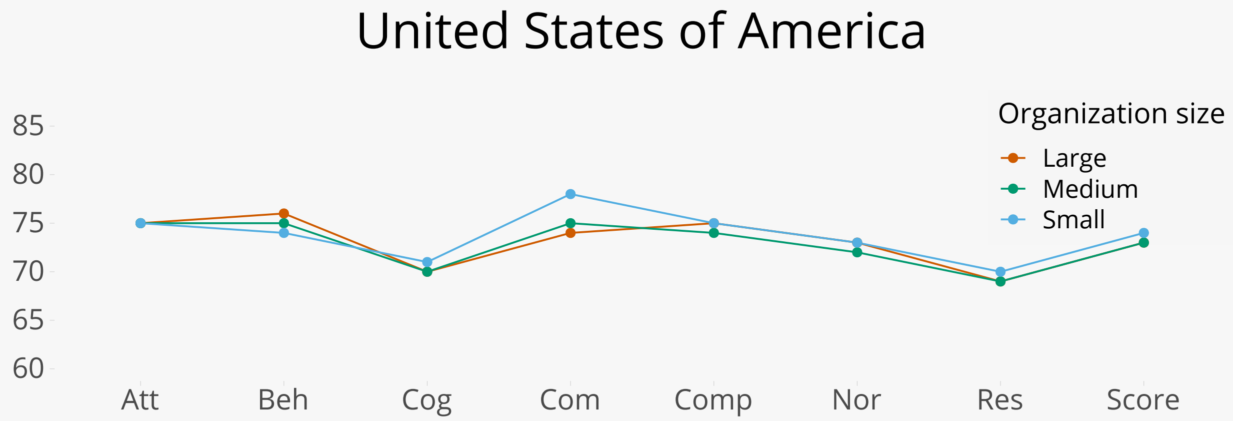


Figure 15: Security Culture in the United States of America as seen by organizational size.

In the USA, we see differences in security culture based on organizational size, where small organizations are outperforming larger organizations. Small organizations are much better at communicating than larger organizations, and have higher levels of Cognition and Responsibility. Large organizations rate the highest when it comes to Behavior. For organizations of all sizes, there are two notable valleys in Cognition and Responsibility. It is our recommendation that organizations assess their employees to identify weak spots in employees' understanding around their role and responsibilities towards security, and implement targeted training and education programs to improve. The USA has a sample size of 1,068 organizations and 177,593 employees.

Security Culture in Oceania

Security culture in Oceania is showing that Australia (73) and New Zealand (72) are quite different from each other, and neither is doing particularly well. It is highly recommended that organizations in this region step up their investments in security awareness, behavior and culture going forward. The other parts of the region are lagging far behind, not even measuring on the Security Culture Index.

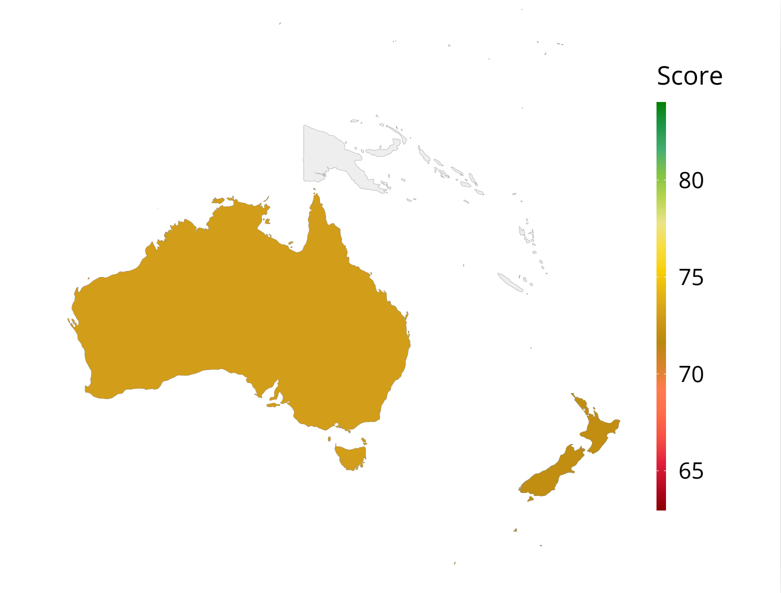


Figure 16: Security culture score in Oceania. The sample size varies from country to country. For more details, please refer to the method section.

Security Culture in Oceania According to Organizational Size

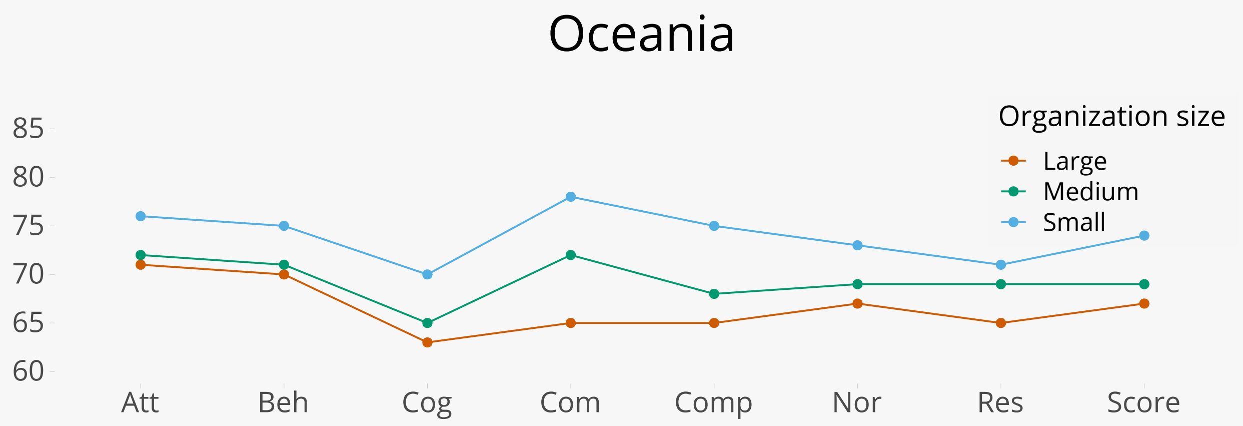


Figure 17: Security culture in Oceania as seen by organizational size.

In the region of Oceania, we noticed that, unlike other regions, none of the lines cross or even meet. We also see that the lines are quite similar in shape, with the main difference being the quality of security culture. Again, we see that Large organizations perform worse on the Communication dimension, while Small organizations outperform the others on all dimensions. Also worth noting is that Large organizations in Oceania perform very poorly on Compliance and Responsibility compared to Europe and North America, suggesting that these two dimensions should be given more attention going forward. The sample size for all of Oceania is 46 organizations and 9,635 employees.

Security Culture in Central and South America

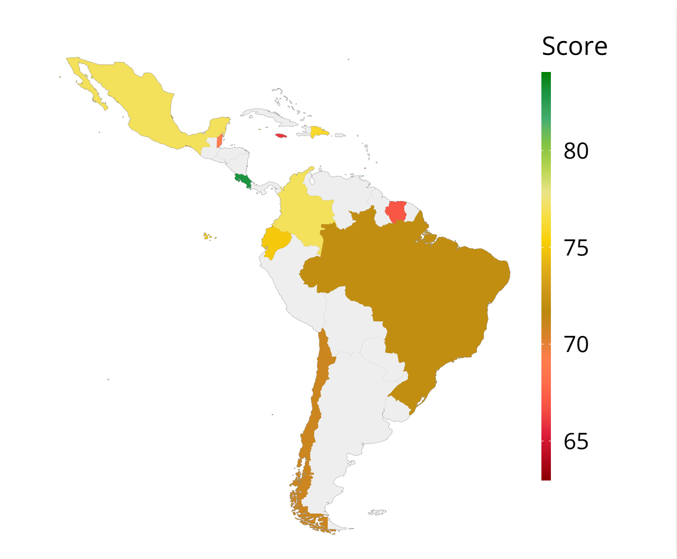


Figure 18: Security culture score in Central and South America. The sample size varies from country to country. For more details, please refer to the method section.

Central American countries show a wide variation of security culture scores, with Mexico performing better than most.

Sample sizes in many Central American countries are low, suggesting that most organizations do not have a minimum level of security measures in place. It is our strong recommendation that organizations in these regions implement adequate security culture measures, including training and assessments.

Most of South America reflected low security culture scores, with the notable exception of Colombia (77). We observe that the continent as a whole is starting to measure security culture, with more countries being added every year. Still, the low sample rate across the continent suggests that there is a long way to go, and organizations need to ramp up their security game.

Security Culture in Central and South America According to Organizational Size

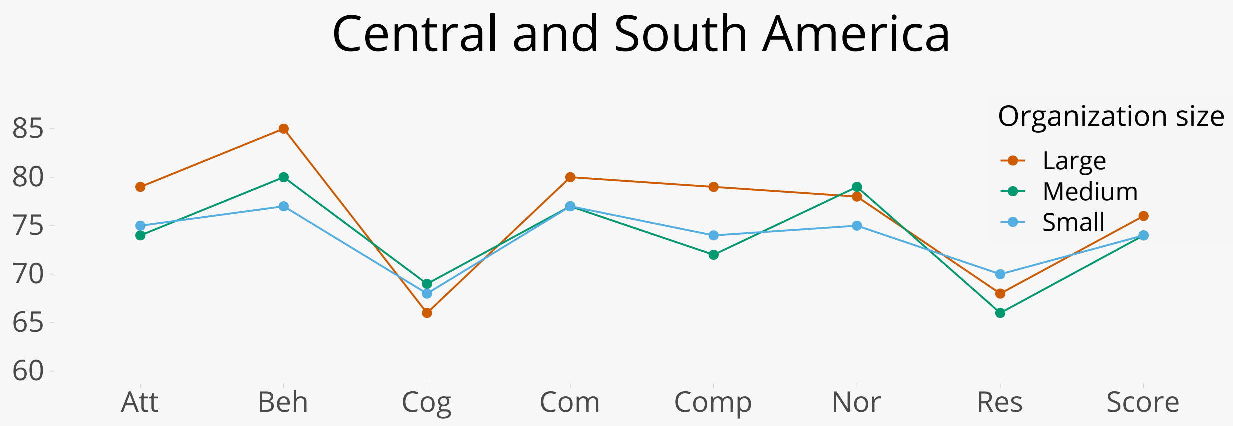


Figure 19: Security culture in Central and South America as seen by organizational size.

Our sample size for Central and South America is 24 organizations and 2,913 employees. The most notable difference in Central and South America is how Large organizations have very large differences between Behaviors (85) and the other dimensions. Further, it is worrying to see how all organizations are struggling with the Cognition and Responsibility dimensions. These very low scores strongly suggest the need for more frequent training and assessments, and a focus on the need for every employee to take security seriously.

Another interesting observation is how in Medium organizations, the dimension of Norms is spiking at 79, much higher than any other region. This is likely due to the sample size, but we will be watching this closely in the future to learn more about why this is appearing.

Security Culture Industry Trends

New to our 2022 report is a comparative view of how security culture trends over periods of time, specifically from 2019-2021. The following snapshots will highlight movement and provide an understanding of how each industry fares on the Security Culture Index (SCI). Comprehensive details of each industry sector can be found on the corresponding Industry Benchmark pages for that industry sector.

Global Trends as Seen Across the Dimensions of Security Culture

When looking at security culture only by its total score, it seems like nothing has changed in the past three years. With a global, average score of 73, security culture seems stagnant. Our ability to measure across the seven dimensions of security culture provides us with a unique perspective into exactly how security culture changes over time, and as can be observed in the figure below, we see that security culture has indeed changed quite a bit since 2019.

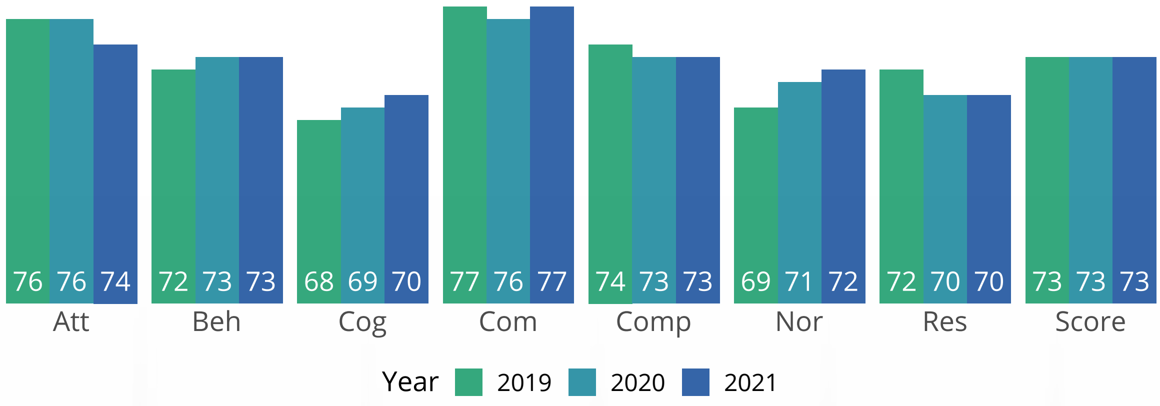


Figure 20: Global trends in security culture.

Using the detailed breakdown, we see improvements in the dimensions of Behaviors, Cognition and Norms. These are all crucial dimensions that look into what employees are learning (Cognition), seeing others do (Behaviors) and their sense of the unwritten rules (Norms) governing security. These three dimensions are closely related, and their influence on each other is strong. This suggests that as more companies are training their employees more frequently, the better security they will achieve.

When examining the other dimensions, the changes are either neutral or negative. Communication seems quite stable and is the best performer across the world. Compliance also seems to be quite stable. However, if we look at Responsibilities, we see a strong drop from 2019 to 2020. When considered along with Attitudes, that also shows a similar size drop, we suggest that organizations focus on making employees feel that they are a strong, positive force that can help secure their workplace against cyber attacks and threats.

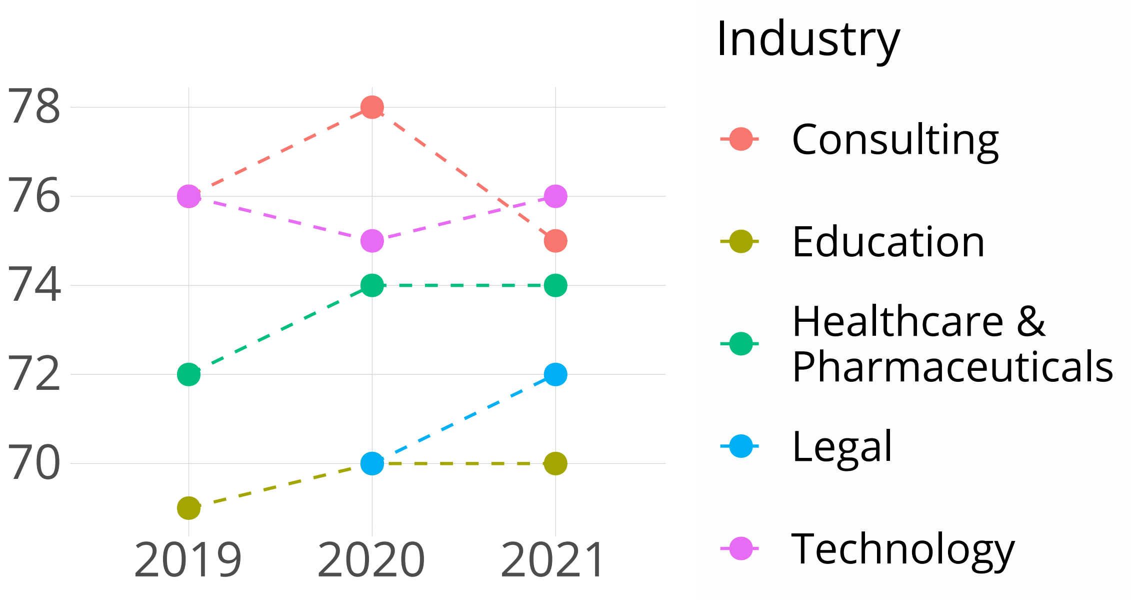


Figure 21: Security culture industry trends.

The Consulting sector continues to show erratic movement in SCS year-over-year, making progress in 2020 (76 to 78), however dropping 3 points to a 75 in 2021. With a sample size of 55 organizations and 10,544 employees, Consulting remains mid-Moderate in rating.

The Education sector had nominal improvement from 2019 to 2020 (69-70), remaining at 70 for 2021. Although the one-point change in score moved this sector from a Mediocre SCI rating to Moderate, more needs to be done to position this sector more favorably. The Education sector represents 50 organizations with 9,081 employees.

Data on the Legal sector was not available in 2019 and although two years of data (2020 and 2021) is not statistically valid in providing trends, we did notice slight favorable movement from 70 to 72. With 20 organizations representing 1,673 employees, we will continue to monitor Legal sector data to mark additional movement within the Moderate SCI range.

The Technology sector, having one of the larger data sets in our research, with 214 organizations and 35,008 employees, continues to maintain a strong Moderate score. With an SCI decrease from 2019 (76) to 2020 (75), the Technology sector regained a score of 76 in 2021.

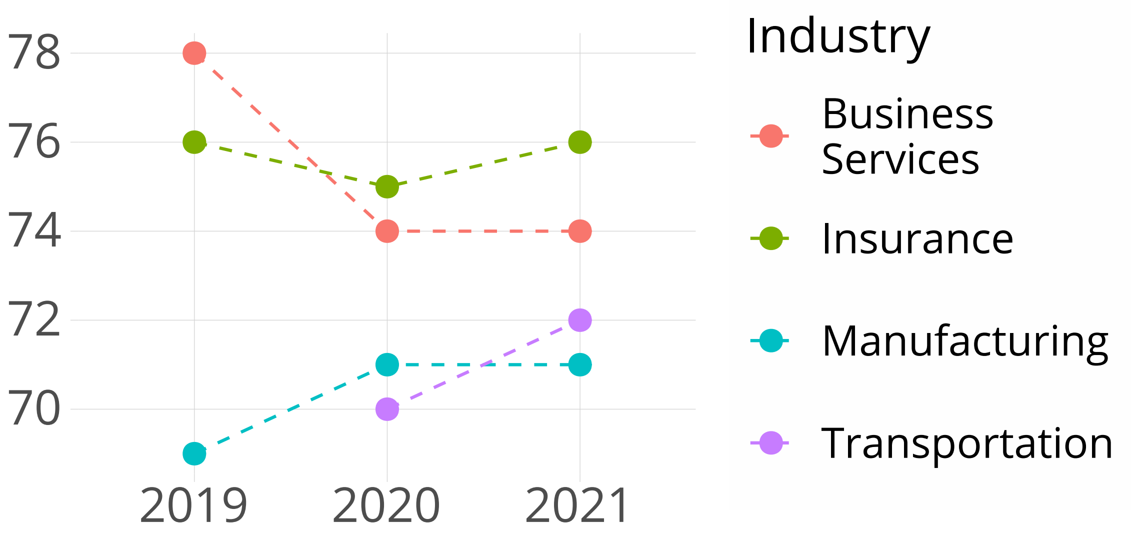


Figure 22: Security culture industry trends.

The Business Services sector experienced a four-point decrease from 2019 (78) to 2020 (74), maintaining a score of 74 in 2021. With a data sample of 102 organizations representing 12,162 employees, the Business Services sector remains in the Moderate range of the SCI.

The Insurance sector experienced a one-point decrease from 2019 (76) to 2020 (75), and regained its score of 76 in 2021. This sector's data represented 52 organizations with 5,194 employees and maintained an SCI rating of Moderate.

The Manufacturing sector, with one of the largest data sets representing 119 organizations with 32,853 employees, remains on the low-Moderate end of the SCI. This sector showed a two-point improvement from 2019 (69) to 2020 (71), maintaining the 71 rating in 2021.

Similar to the Legal sector, data was not available in 2019 for the Transportation sector. Although two years of data (2020 and 2021) is not statistically valid in providing trends, we did notice slight favorable movement from 70 to 72. With 32 organizations representing 6,867 employees, we will continue to monitor Transportation sector data to mark additional movement within the Moderate SCI range.

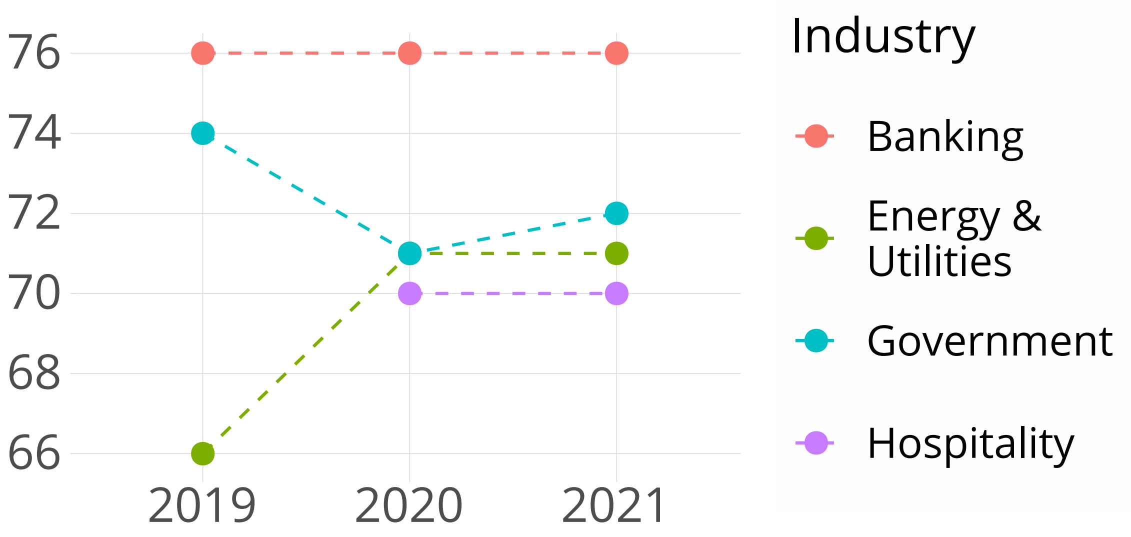


Figure 23: Security culture industry trends.

The Banking sector maintains an SCI score of 76 for the third year (2019-2021). Holding steady in the mid-Moderate range, this sector had a data set of 105 organizations representing 14,184 employees.

The Energy and Utilities sector experienced a five-point increase from 2019 (66) to 2020 (71) maintaining an SCI score of 71 in 2021. Although the movement from 2019-2020 increased their rating from Mediocre to low-Moderate, a stronger security culture is expected due to the critical nature of this sector. The data set represented 62 organizations with 10,590 employees.

Data on the Hospitality sector was not available in 2019 and although two years of data (2020 and 2021) is not statistically valid in providing trends, this sector remained at a 70. With nine organizations representing 2,233 employees, we will continue to monitor Hospitality sector data to mark additional movement within the Low-Moderate SCI range.

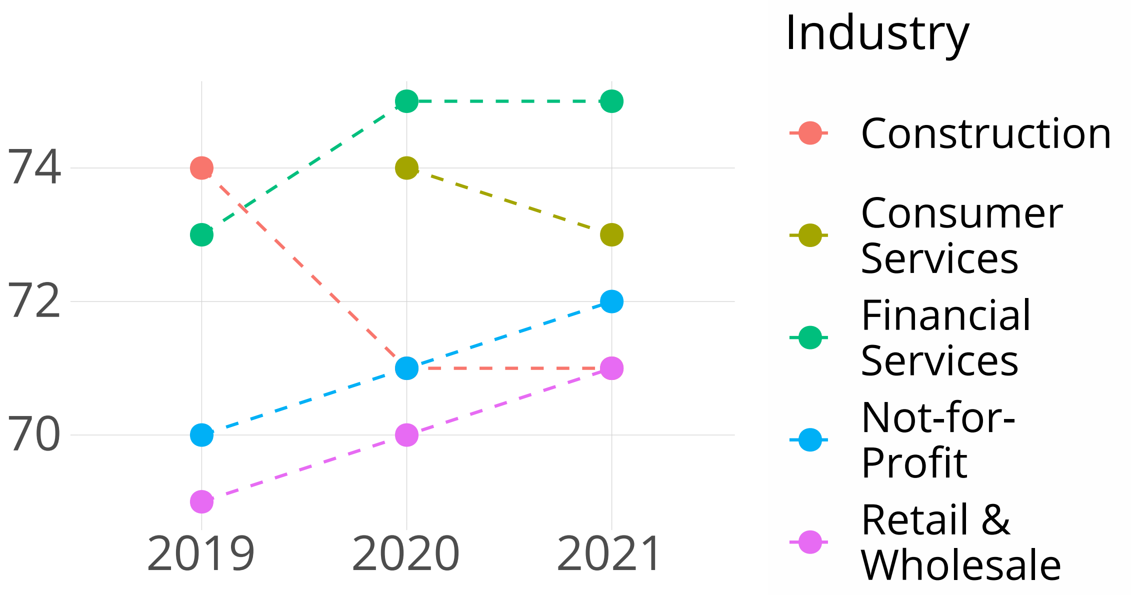


Figure 24: Security culture industry trends.

The Construction sector dropped three points from 2019 (74) to 2020 (71) and has maintained the low-Moderate SCI rating of 71 for the second year. This sector's data set represented 35 organizations with 4,797 employees.

Data on the Consumer Services sector was not available in 2019 and although two years of data (2020 and 2021) is not statistically valid in providing trends, this sector moved from a 74 (2020) SCI to a 73 (2021). With 33 organizations representing 3,597 employees, we will continue to monitor Consumer Services sector data to mark additional movement within the mid-Moderate SCI range.

The Financial Services sector had a two-point increase from 2019 (73) to 2020 (75) and maintains an SCI score of 75 in 2021. This sector stands firm with a mid-Moderate rating and represents 187 organizations with 26,853 employees. The Financial Services sector has one of the largest data sets in this research.

The Not-for-Profit sector showed a steady increase year-over-year in SCI rating 70 in 2019, 71 in 2020 and 72 in 2021. With 74 organizations representing 10,509 employees, the Not-for-Profit sector remains in the low-Moderate SCI range.

The Retail and Wholesale sector also showed a steady increase year-over-year in SCI rating 69 in 2019, 70 in 2020 and 71 in 2021. Remaining in the low-Moderate range, this sector data represents 73 organizations with 25,776 employees.

*Our ability to measure across the **seven dimensions of security culture** provides us with a unique perspective into exactly how security culture changes over time...*

*...We see that **security culture has indeed changed quite a bit since 2019**.*

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.

Benchmark Overview

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

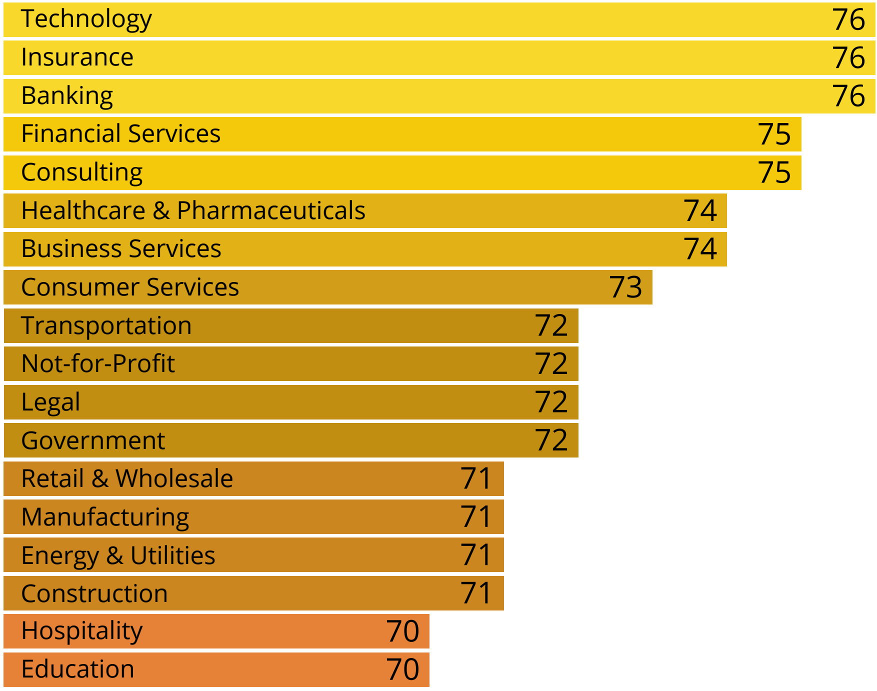


Figure 25: Security Culture Benchmark.

This overview provides direct insights into the difference across the industry sectors and allows for you to compare your organization to others. You can also use this section to compare your industry score with other industry sectors.

Industry Benchmark

Compared to previous years, we see that the worst performing sector of Education now has moved into the Moderate security culture range, with its score of 70. The same is true with the Energy and Utilities, Manufacturing, and Retail and Wholesale industries. This is great news, as it means that there are no industry sectors that show Poor or Mediocre security culture. This is the first time we have not reported industries with a Poor or Mediocre security culture. Worryingly, not much improvement is seen on the other end of the spectrum. Instead, some sectors show a decline in security culture, most notably Business Services, with a drop from 78 in 2019 to their current score of 74.

Banking

76

14,184

105

Banking institutions experienced an increase in cyber attacks, which elevate operational risks. Many of these attacks continue to utilize phishing emails to obtain remote access to conduct ransomware or business email compromise attacks. The pandemic's impact continues to reverberate throughout the banking sector as the industry adapts to additional compliance obligations. In November 2021, the federal government ruled that banking organizations must notify their primary federal regulator within 36 hours in the event of certain types of computer security incidents. Additionally, 2021 brought the conclusion of COVID-19-related assistance programs. These adjustments can provide opportunities for new social engineering attempts against banking infrastructure. The industry's consistent Security Culture Score of 76 bodes well for their approach to overall risk management strategy and defense against emerging threats.

Survey results reveal a number of areas in which the Banking sector has improved with minor, positive shifts in multiple dimensions. In the past year, the Norms dimension increased by two points (74) while both Behavior (78) and Communication (78) also increased by a single point, consistent with the Banking industry's history of strong communications channels. Responsibility (72), Cognition (73) and Compliance (79) are consistent with last year's report. All scores remain in the Moderate range.

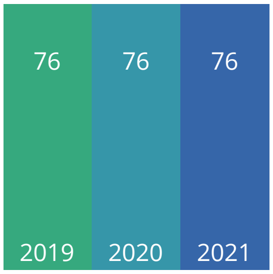


Figure 26: Security culture trends in Banking.

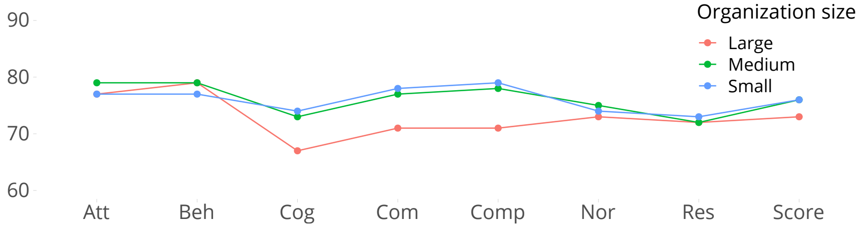


Figure 27: Security culture in Banking according to organizational size.

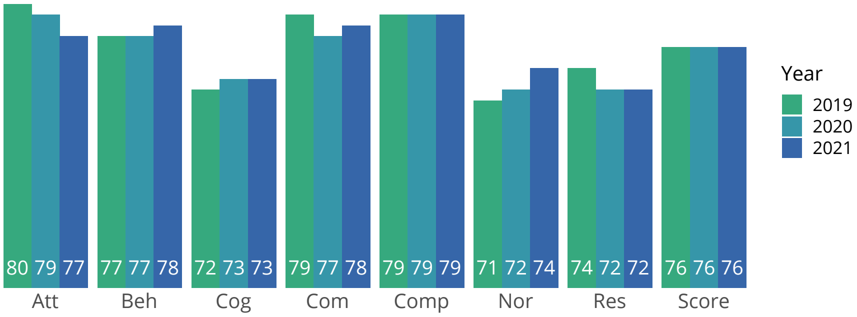


Figure 28: Trends as seen across the dimensions of security culture in Banking.

Areas for Improvement

The only area for improvement—the Attitudes dimension—experienced a downward trend over the last three years from 80 to 77. This may be attributed to ongoing "COVID-19 exhaustion" as the industry continues to manage personnel hybrid working and the ongoing safety protocols required for in-person operations. Banking sector security advocates can reverse this trend through targeted security awareness campaigns spearheaded by senior leadership, and focused on the vital role everyone plays in protecting high value financial data and maintaining a strong security culture.

Business Services

74

12,162

102

The Business Services sector represents a wide range of organizations typically offering assistance in areas such as office administration, physical security, waste disposal, cleaning services and hiring/placing personnel, which makes for an interesting mix in overall measurement of descriptive statistics. As an industry historically prone to a high percentage of targeted phishing attacks, we saw the Security Culture Score remain constant this year at a moderate 74. In an industry built heavily on relationships, the threat of a cyber attack could potentially damage existing customer relationships, disrupt customer loyalty and prevent new business opportunities.

The dimension of Behavior remained unchanged this year at 74, still considered Moderate on the scale. The Cognition dimension also remained unchanged at 71, and although is in the low-Moderate range, is close to falling to Mediocre. If organizations within the Business Services sector fail to provide their employees with the necessary tools to best understand how and why they should be more security aware, then the Behavior dimension will certainly be negatively affected. Survey results also reflect a one-point increase in the Norms dimension (from 73 to 74), indicating that employees have the capacity to uphold unwritten rules of conduct when trained to do so.

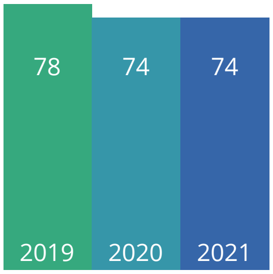


Figure 29: Security culture trends in Business Services.

Areas for Improvement

The Business Services industry saw declines in the following dimensions in 2021: Attitude (76 to 75), Communication (80 to 78), Compliance (75 to 74) and Responsibility (72 to 71). Although most of these downward trends seem nominal, as a whole, they indicate that there are inherent challenges in demonstrating an eagerness and commitment to improvement.

A strong commitment to comprehensive and continuous training and education will favorably impact these scores and position the organizations within this industry to create a stronger security culture. Increased training and awareness will help strengthen employee understanding and buy-in for security-related behaviors and values.

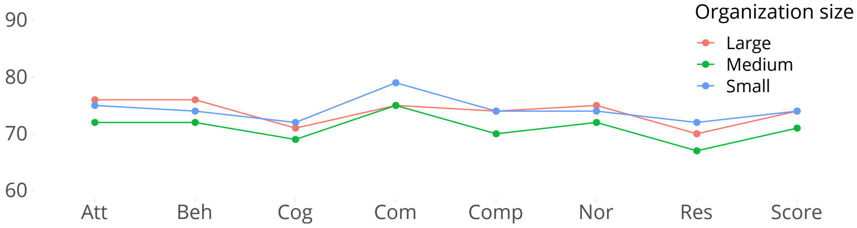


Figure 30: Security culture in Business Services according to organizational size.

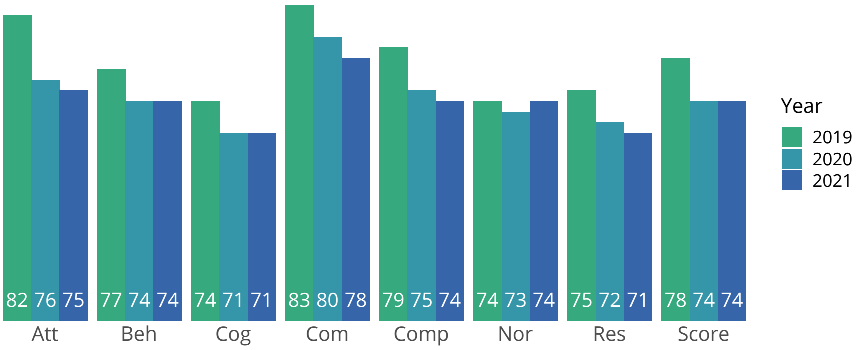


Figure 31: Trends as seen across the dimensions of security culture in Business Services.

Construction

71

4,797

35

The Construction sector continues to face hardships due to pandemic-related delays of the most basic goods and materials needed to conduct their operations. Their overall supply chain continues to be challenged by inflexible business operations and practices, political indecision and continued shortage of trained labor. This, coupled with the ease at which ransomware attacks occur, makes this industry an obvious and attainable target. The Construction sector, which often includes a complex collection of contractors (both supply chain and on-site), scored a low-Moderate 71, however is increasingly close to falling into the Mediocre portion of the scale.

The only dimension to see an increase from last year is Norms (70 to 71). This increase does not stand out as favorable because the score still ranks at the very bottom of the Moderate range. Cybercriminals will continue to attack industries they know are vulnerable. Construction organizations need to carefully evaluate their ability to drive favorable movement across all dimensions, leading the charge with awareness and training.

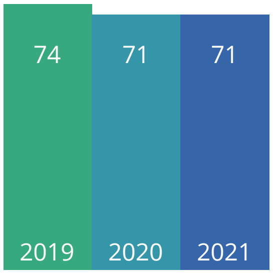


Figure 32: Security culture trends in Construction.

Areas for Improvement

The Construction industry saw declines in five dimensions in 2021: Attitude (72 to 71), Behaviors (72 to 71), Communication (77 to 76), Compliance (72 to 71) and Responsibilities (69 to 68). Although Cognition held steady at 67, it remains their lowest score. Many work environments in this industry are not conducive to traditional computer-based training because much of the workforce is widely dispersed on job sites without access to computers and/or centrally managed, handheld devices. Options with mobile training continue to improve, but have not yet been universally embraced and deployed. The Construction industry needs to continue finding non-traditional ways (including mobile-first options) to drive awareness and raise employees' levels of readiness to detect cyber attacks.

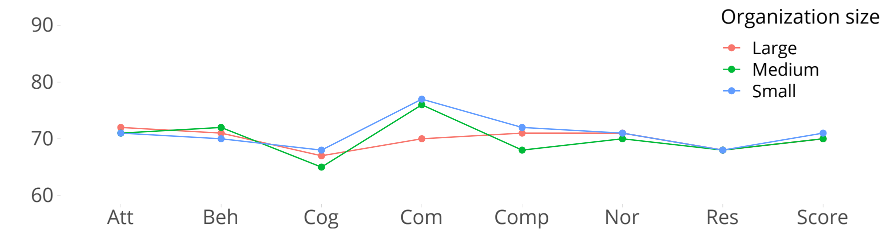


Figure 33: Security culture in Construction according to organizational size.

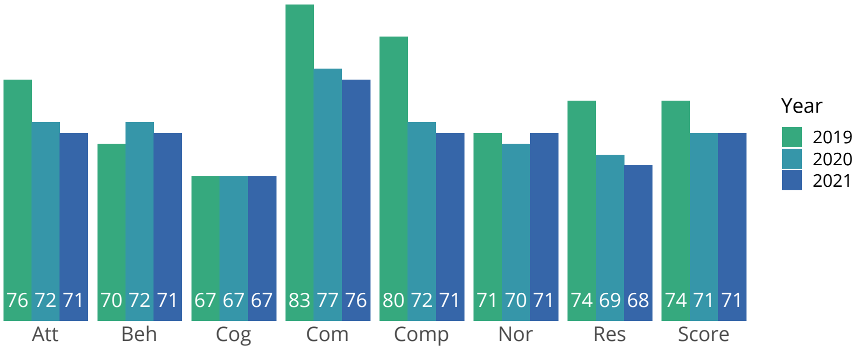


Figure 34: Trends as seen across the dimensions of security culture in Construction.

Consulting

75

10,544

55

The Consulting sector, with an overall security culture score of 75, continues to be a very attractive, high-profile target for cybercriminals. In August 2021, one of the largest global consulting groups, was hit with a massive $50 million ransomware attack by the group LockBit with help from an internal source (insider threat). The reputation and brand damage that this very public attack brings is staggering.

Consulting companies are data rich, and clients expect elevated levels of confidentiality, which may prove challenging with the high-paced and stressful environment in this sector. This industry dropped in every dimension since last year, yet their scores are still favorable at mid-high Moderate. The strongest scores were in Communication (79) and Attitude (76). With Communication being a cornerstone in the Consulting sector, it is likely that employees understand their respective roles and what is expected of them relative to securing their environment.

Areas for Improvement

The two lowest dimensions for the Consulting industry are Responsibilities (72) and Cognition (73). With Cognition, it is likely that employees possess adequate understanding of what their roles and responsibilities are regarding driving a more secure culture. Employees know that they need security training, but the program should deploy content at the right time, in the right way, to the already receptive audience. The challenge is not whether they understand their role, it is if they perceive their role as a critical element in preventing a cyber attack. Leaders need to ensure that their employees can make the leap from "understanding" to "doing" through continued and comprehensive awareness and training engagement.

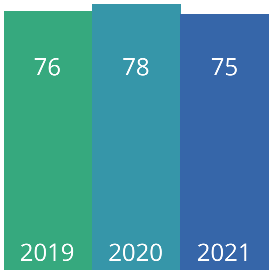


Figure 35: Security culture trends in Consulting.

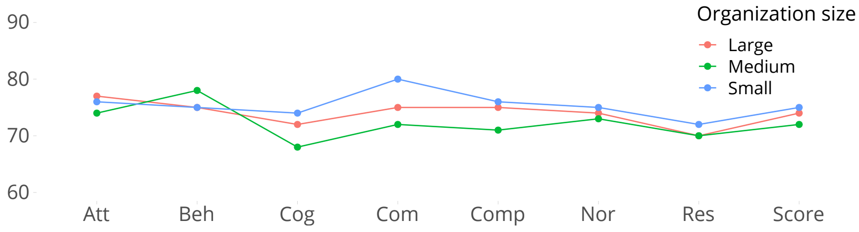


Figure 36: Security culture in Consulting according to organizational size.

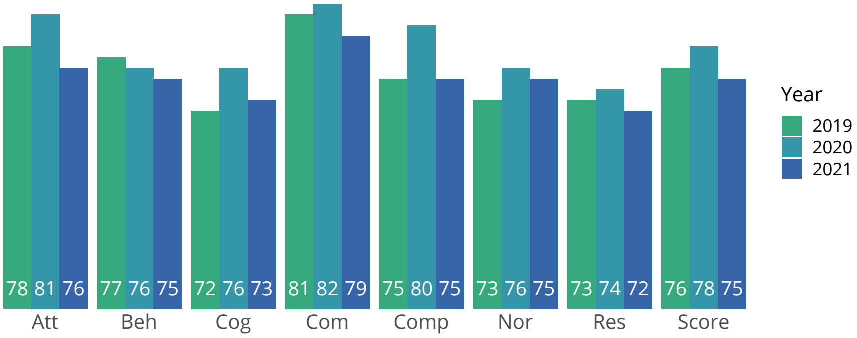


Figure 37: Trends as seen across the dimensions of security culture in Consulting.

Consumer Services

73

3,597

33

The Consumer Services industry has an overall security culture score of 73. Organizations in the Consumer Services sector typically offer support-based products that are not physical in nature, making for an interesting mix in overall measurement of descriptive statistics. Companies in this sector are traditionally behind in the adoption of new technology and upgrading their overall security infrastructure/operations and are often seen as attractive targets by cybercriminals due to their reduced resilience to attack.

Although this sector experienced drops in every dimension with the exception of Norms (72 to 73), they still have Moderate scores in the following: Attitude (74), Behavior (73), Communication (78) and Compliance (73). Based on these scores, organizations in the Consumer Services industry should harness the positive attitudes their employees have, coupled with their willingness to behave in a more security-minded fashion. Having a dispersed workforce requires these organizations to use creative techniques to pull employees into a place where they feel like part of the overall team.

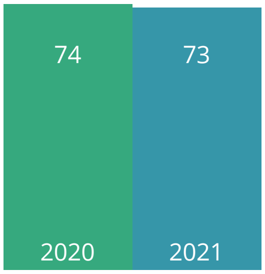


Figure 38: Security culture trends in Consumer Services.

Areas for Improvement

The two dimensions that reside within the Mediocre portion of the scale are Cognition (69) and Responsibilities (69). The ongoing pandemic continues to challenge Consumer Services organizations because their workforce is still heavily shifting to work from home, and in an industry that struggles with updated technology, that combination of distraction and weakened defenses are an attractive target for cybercriminals. Additionally, if employees are remote and without proper training and technology, they cannot operate as an integral part of the human firewall. Furthermore, they likely will not be equipped to translate that role into personal responsibility and the actions that they must take to be more security ready.

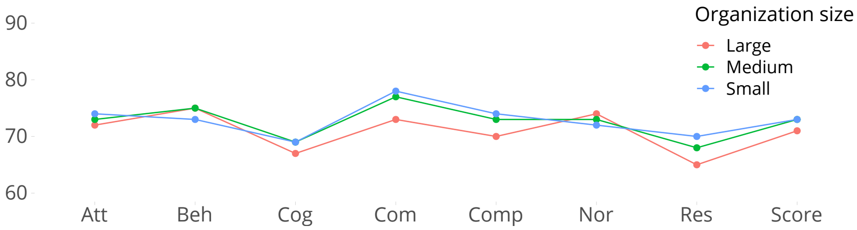


Figure 39: Security culture in Consumer Services according to organizational size.

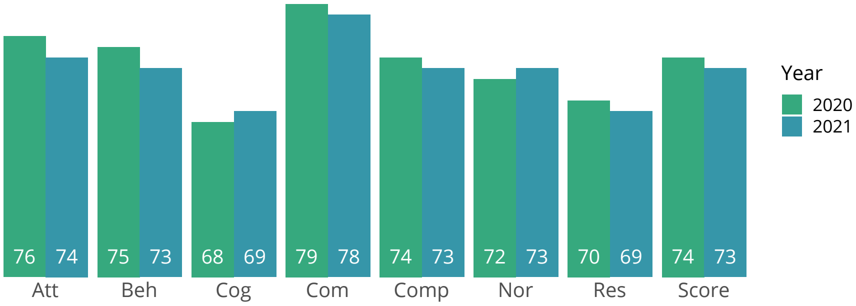


Figure 40: Trends as seen across the dimensions of security culture in Consumer Services.

Education

70

9,081

50

Cyber attacks on schools and colleges, particularly targeting kindergarten through twelfth grade (K-12) institutions, have grown more frequent during the pandemic due to their increased reliance on technology. Public school systems often face limited budgets for cybersecurity tools, training and other resource constraints which make them an inviting target of ransomware attacks which can render systems inoperable. These attacks have also resulted in theft of confidential student data and the disruption of distance learning services. This increased threat environment requires that "educational leadership, information technology personnel and security personnel will need to balance this risk when determining their cybersecurity investments." Educational institutions maintained last year's Security Culture Score of 70, a score on the verge of falling down into the Mediocre range, which underscores the need for increased investment in several aspects of security culture.

Norms saw a noteworthy increase of two points (70) while Cognition also increased to 68, a one-point difference over last year. Behavior (69) and Communication (73) remained consistent with last year's scores.

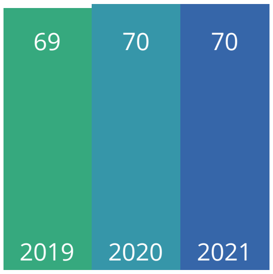


Figure 41: Security culture trends in Education.

Areas for Improvement

The Attitudes dimension (73) has maintained its downward trend for the third year in a row and Responsibility (67) has taken a slight downturn one point from last year's survey, both are likely attributable to "COVID-19 exhaustion." With increased funds for COVID-19 testing and hygiene protocols, and if schools maintain their return to in-person status, we can expect these dimensions will return to their pre-pandemic scores. As with last year, Education ranked last (along with Hospitality) in our industry comparisons. The incremental improvements noted above indicate the Education sector is moving in the right direction towards improvements in security culture.

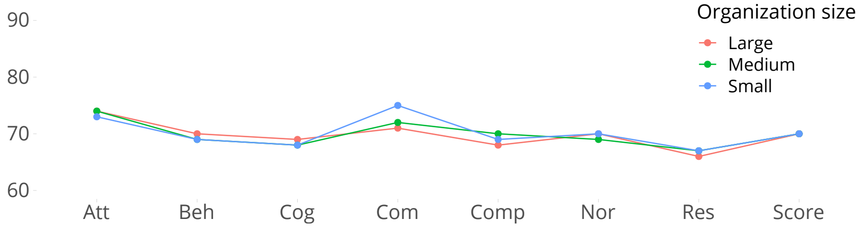


Figure 42: Security culture in Education as seen by organizational size.

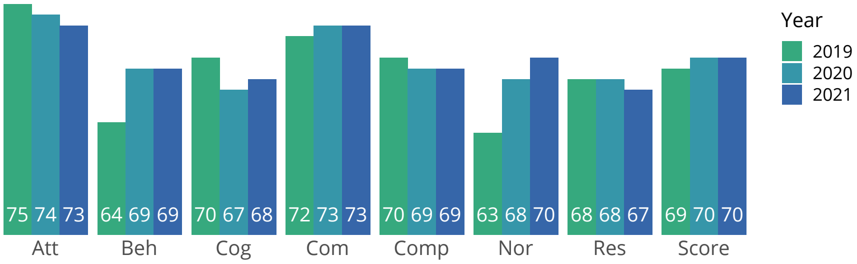


Figure 43: Trends as seen across the dimensions of security culture in Education.

Energy and Utilities

The critical nature of Energy and Utilities was the subject of international headlines in the Spring of 2021. This was due to the largest cyber attack on an oil infrastructure target in the history of the United States, the Colonial Pipeline. In response, many companies in the sector sought cyber insurance coverage amid increased engagement with government regulators[1]. In addition, the National Institute of Standards and Technology (NIST) published updated guidelines to help organizations align compliance and security programs to better manage risk[2]. The incident also highlighted the criticality of security planning and incident response across private and public sectors, which likely contributed to the increases in multiple security dimensions this year. The industry's overall Security Culture Score remains steadfast at a low-Moderate 71.

Four of the seven dimensions measured showed incremental improvement over last year's survey. Behaviors (72), Cognition (67), Compliance (72) and Norms (70) have increased by one point but are either in or moving towards the Mediocre range. Communication remains the industry's strongest dimension at 75.

71

10,590

62

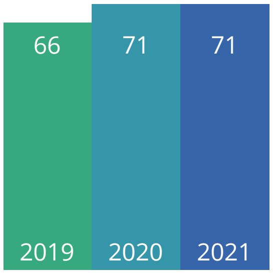


Figure 44: Security culture trends in Energy and Utilities.

Areas for Improvement

The Attitudes dimension dropped from last year, down from 74 to 72, which may be attributed to the negative effects on industry morale by the high profile nature of recent ransomware attacks. As noted in previous Security Culture Reports, the Energy & Utilities sector has much room for improvement. This year, it is ranked in the bottom, only one point behind Education and Hospitality at 70. While incremental improvement has occurred in the last year, the vital nature of this sector necessitates a greater emphasis on continuous security training and testing, while providing constructive feedback to employees.

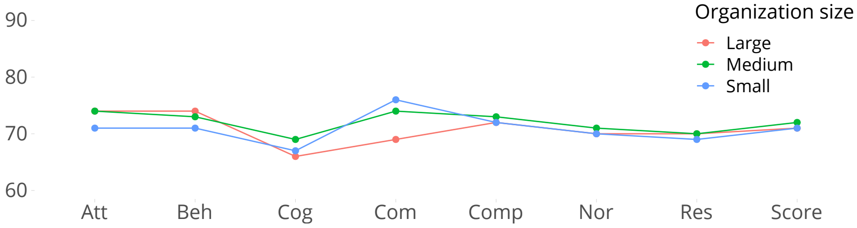


Figure 45: Security culture in Energy and Utilities according to organizational size.

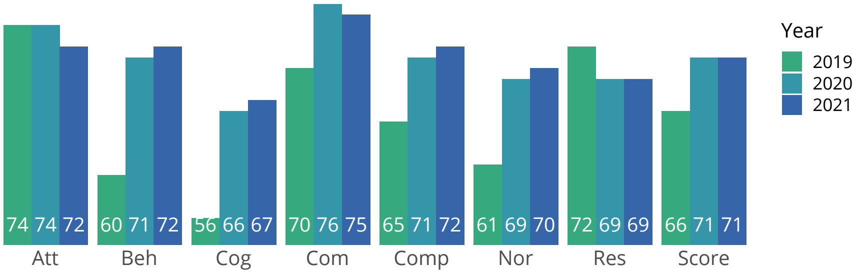


Figure 46: Trends as seen across the dimensions of security culture in Energy and Utilities.

[1] https://www.dhs.gov/news/2021/07/20/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators

[2] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.09292021.pdf

Financial Services

75

26,853

187

The Financial Services sector maintained their Moderate Security Culture score of 75, and continues to have strong Moderate scores across each dimension. Within this industry, controlling trades and governing significant amounts of money while housing highly confidential financial and personal client information, makes them a high value target. The past few years have been painful for the Financial Services sector, with Experian experiencing a loss of 24 million customers and 800,000 business records, and Capital One losing 100 million credit card applications[1]. These are just two of the many Financial Services companies that have been successfully compromised.

As companies in this sector continue to adapt to new pandemic-era remote and hybrid working conditions, the safety of normal business functions remains under scrutiny. Cyber attacks will not stop in this sector. Financial Services organizations need to adopt robust, multi-layered defense strategies and immerse their employees in comprehensive and continuous security awareness training to increase employee resilience to social engineering attacks. The highest scoring dimensions were Communication (78), Attitude (77), Behavior (77) and Compliance (77), highlighting that engaged employees believe, behave and follow security policies.

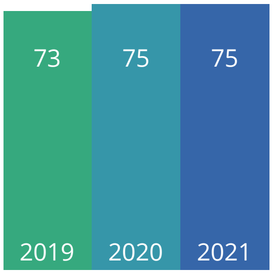


Figure 47: Security culture trends in Financial Services.

Areas for Improvement

The least favorable dimensions of the Financial Services industry are Responsibilities (72) followed by Cognition (73). Cybercriminals continue to exploit organizations with untrained users, lower comprehension levels and click-happy employees. If an employee's overall understanding is low, then there is a high probability that they lack needed resilience in the face of a cyber attack. Security awareness training combined with ongoing simulated phishing tests are critical to help employees build the muscle memory and gut instincts needed to sort the good from the bad.

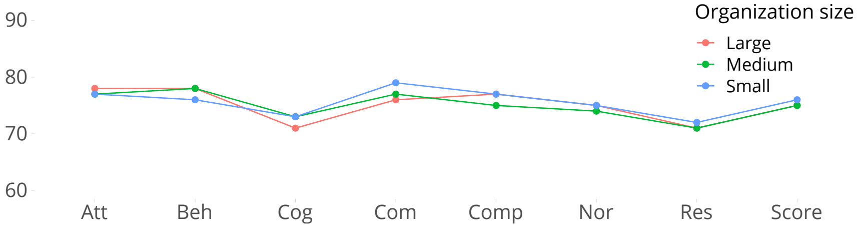


Figure 48: Security culture in Financial Services according to organizational size.

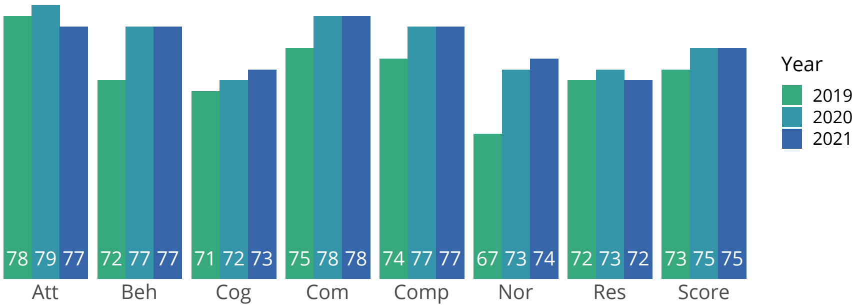


Figure 49: Trends as seen across the dimensions of security culture in Financial Services.

[1] https://www.upguard.com/blog/biggest-data-breaches-financial-services

Government

72

20,505

120

At the federal level, the Department of Defense (DoD) released their Cybersecurity Maturity Model Certification (CMMC) for use in assessing the cybersecurity environment of DoD's vendor supply chain. Additionally, the National Institute of Standards and Technology (NIST) continues to update enterprise risk management[1] guidance on how federal agencies should utilize the Cybersecurity Framework[2]. State and local governments face the challenges of a multi-tiered regulatory environment and an expanding attack surface. Although recent legislation allocated billions of dollars in cybersecurity[3] funding from this grant program, it will take time for the funds to make their way to intended recipients. There were improvements in several dimensions, resulting in a slight increase to a low-Moderate 72 score.

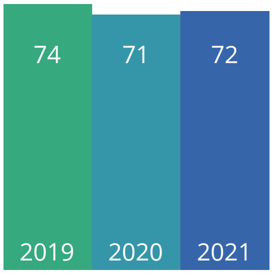


Figure 50: Security culture trends in Government.

The noteworthy improvement of five out of seven dimensions throughout the government is likely due, at least in part, to the high profile nature of the SolarWinds-related malware attack. In December 2020, the U.S. government issued an Emergency Directive in response to a known compromise involving SolarWinds Orion products. The attack was unprecedented and a "significant cyber incident impacting enterprise networks across federal, state, and local governments, as well as critical infrastructure entities and other private sector organizations".[4] This intrusion was subsequently attributed to the Russian Foreign Intelligence Service (SVR)[5]. That a foreign intelligence service targeted local-level networks, impacted awareness throughout the Government sector. Three dimensions improved by two points—Behavior (73), Cognition (69), Compliance (74)—while Communication (76) and Norms (71) increased by one.

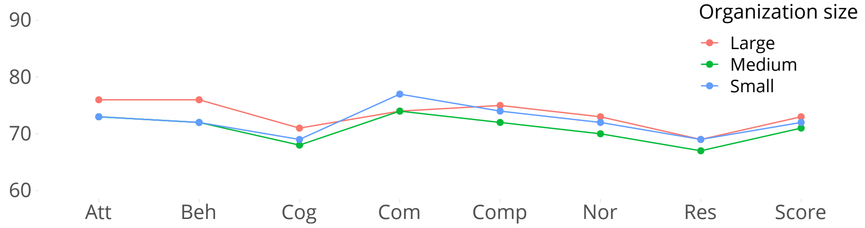


Figure 51: Security culture in Government as seen by organizational size.

Areas for Improvement

The Attitude (74) dimension, though traditionally the strongest dimension among Government, was unchanged from last year's survey. The Responsibility (68) dimension, traditionally the weakest, also remained unchanged. The Government workforce can gain a stronger sense of responsibility for security culture by leveraging additional training and awareness to educate users on threats by foreign intelligence services and other bad actors against federal, state and local infrastructure.

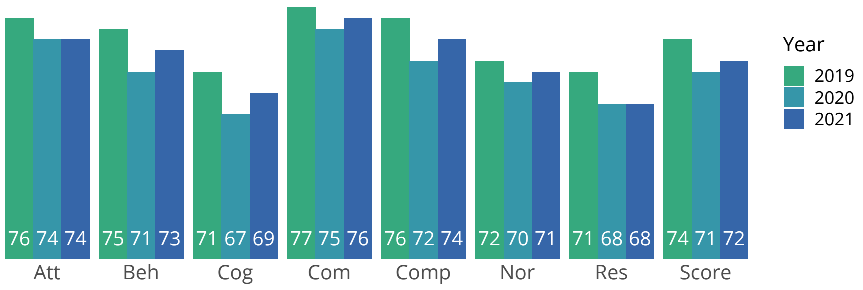


Figure 52: Trends as seen across the dimensions of security culture in Government.

[1] https://csrc.nist.gov/publications/detail/nistir/8286c/draft
[2] https://csrc.nist.gov/publications/detail/nistir/8170/final
[3] https://www.congress.gov/bill/117th-congress/house-bill/3684/text
[4] https://www.cisa.gov/supply-chain-compromise
[5] https://www.cisa.gov/uscert/sites/default/files/publications/CISA_Fact_Sheet-Russian_SVR_Activities_Related_to_SolarWinds_Compromise_508C.pdf

Healthcare and Pharmaceuticals

74

24,761

114

Healthcare and Pharmaceuticals organizations have long been vigilant in the protection of intellectual property and financial information. However, the rapidly expanded use of telemedicine has increased the amount of data available through patient and healthcare provider portals and apps. These changes in provider/patient use of technology result in an increased attack surface; this can impact data ranging from personally identifiable information (PII) to intellectual property (IP), such as extremely valuable drug research efforts. Moreover, medical identity theft, which often includes both a patient's social security and credit card number(s), are highly lucrative endeavors for cybercriminals. Compounding the threat is a need for medical providers to maintain immediate access to patient data; institutions often pay a ransomware attacker to regain access, which also makes this industry an attractive target to malicious actors. The industry's overall results remain consistent over the last two years, with a Moderate Security Culture Score of 74.

Last year's Security Culture Report noted a need for improvement in the Norms dimension, which measures the unwritten rules related to security expectations and how employees are adopting them. This year, Norms (74), as well as Cognition (72) improved by two points. The Behavior dimension (76) also improved by one point. Although consistent with last year's scores, Attitude and Communication maintain a strong showing (77).

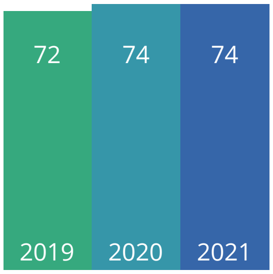


Figure 53: Security culture trends in Healthcare and Pharmaceuticals.

Areas for Improvement

The Responsibility (70) and Compliance (74) dimensions remain unchanged. There are several opportunities for improvement, particularly Responsibility, which is on the verge of dropping into the Mediocre range of the scale. This dimension measures an employee's understanding of the safeguards they provide, as those safeguards relate to their organization's security posture, which is required by federal and state regulations to include the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The industry would benefit from additional training to understand how professional security measures translate into a safer personal home environment as well.

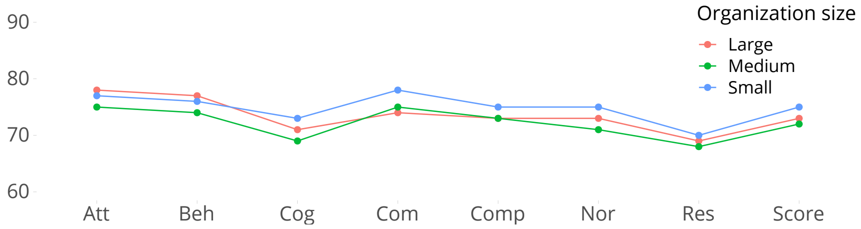


Figure 54: Security culture in Healthcare and Pharmaceuticals according to organizational size.

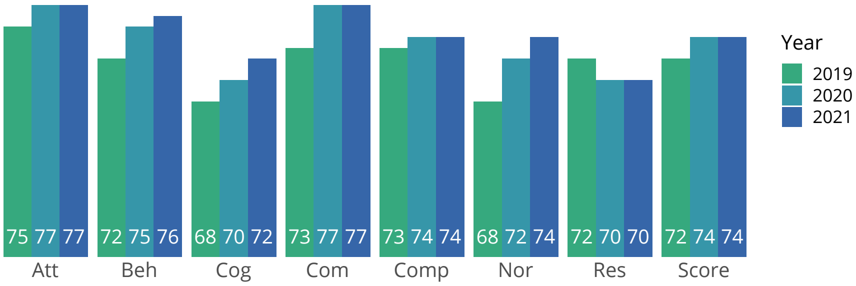


Figure 55: Trends as seen across the dimensions of security culture in Healthcare and Pharmaceuticals.

Hospitality

70

2,233

9

In past years, the Marriott chain, The Ritz London hotel, MGM Resorts and Choice Hotels International were hit with major security breaches[1]. This is just a sample of the many breaches that occurred in the Hospitality industry. In these cases, cybercriminals were looking for private information (i.e., credit card, emails and other personal data) of guests' booking reservations through online portals, check in/out and meal services. Additionally, with the sheer volume of people going in and out of hotels and restaurants, it is difficult to keep track of authorized access for employees and guests, making it easier to infiltrate physical environments.

With an overall security culture score of 70, the Hospitality industry maintains its spot as a preferred target and joins Education for the lowest Security Culture Score.

There is a three-way tie of the highest rated dimensions: Attitude (73), Behavior (73) and Communication (73), but still at low-Moderate on the scale. These scores make it clear that employees have a strong willingness to help build and be part of a more secure culture. Through communication and job-specific awareness and training, employees can raise their readiness levels to spot different physical and cybersecurity threats.

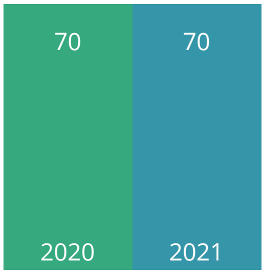


Figure 56: Security culture trends in Hospitality.

Areas for Improvement

Cognition (66) is the lowest ranked dimension with Compliance and Responsibilities not far behind at 67. More frequent and consistent training is needed to ensure that employees understand what the inherent risks are within their respective environments and what steps they can take to mitigate those risks. Understanding, coupled with enacting policies and guidelines that outline what is expected, will help minimize the current gap. Hectic work environments need security aware employees.

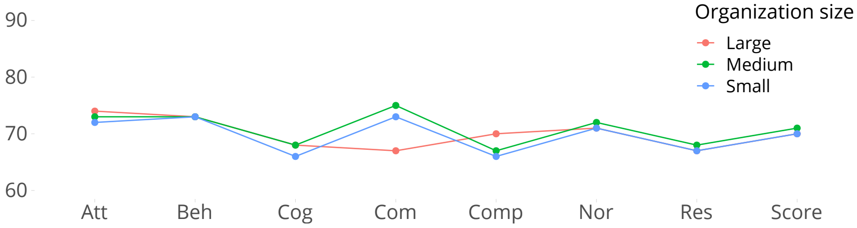


Figure 57: Security culture in Hospitality as seen by organizational size.

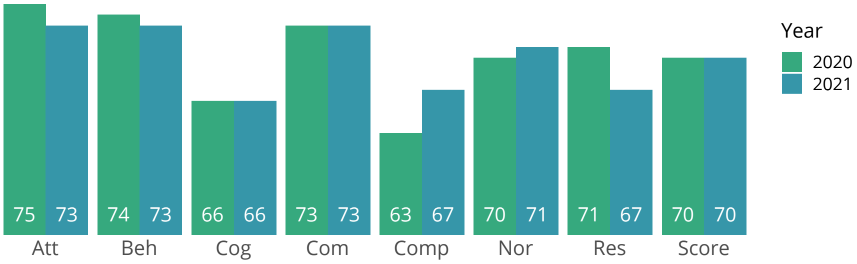


Figure 58: Trends as seen across the dimensions of security culture in Hospitality.

[1] https://www.upscalelivingmag.com/5-recent-luxury-hotel-data-breaches-you-should-know-about/

Insurance

76

5,194

52

Cyber attacks in the Insurance segment continue to grow due to the amount of personal, financial and medical information retained by these organizations. In contrast to other sectors, which hold mainly sensitive financial data, insurers typically also collect a large amount of protected personal sensitive information[1]. In March 2021, one of the largest insurers, CNA Financial Corp., paid $40 million in ransom to reclaim control of their networks after a targeted cyber attack.[2]

The Insurance sector has some of the highest dimension scores across all of the industries surveyed. With an overall score of 76, the following dimensions are among their highest: Communication (80), Attitude (78) and Compliance (77). Communication and Compliance are key in this industry. Employees need to understand and always adhere to security policies. Additionally, this is a highly regulated industry and insurers need to make certain that they always meet regulatory standards. Additionally, having accurate and timely information to respond to policyholders is critical in order to promote assurance in their business transactions.

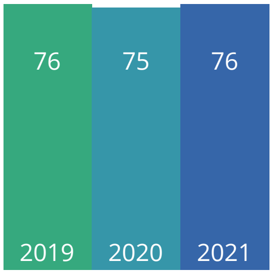


Figure 59: Security culture trends in Insurance.

Areas for Improvement

The lowest dimension score is Responsibilities at a Moderate 73. In Perry Carpenter's book, *Transformational Security Awareness*, Carpenter notes, "Just because I am aware, doesn't mean that I care."[3] Meaning, employees could be following security policies and understand their role in better securing the organization, but still may not care. Making a strong connection between what they need to know and do, and how this knowledge will benefit them personally, is a strong recipe to gain buy-in.

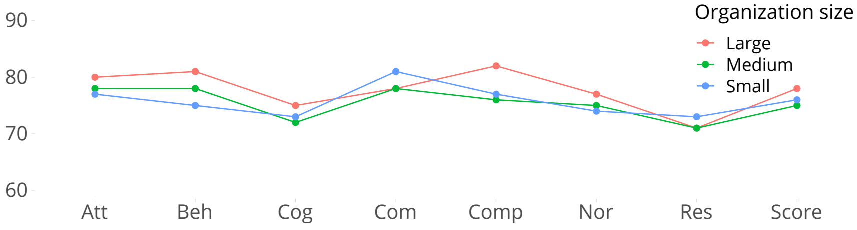


Figure 60: Security culture in Insurance according to organizational size.

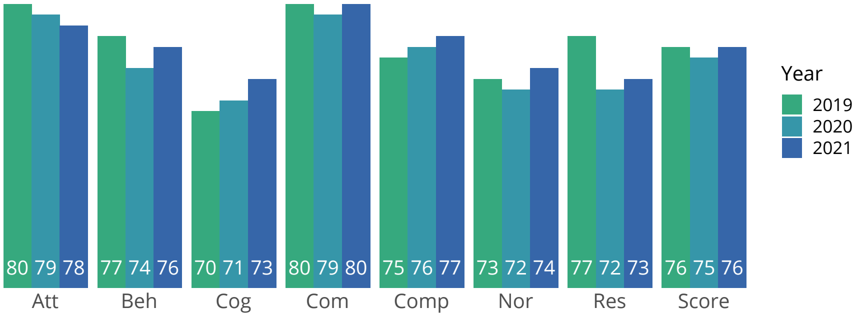


Figure 61: Trends as seen across the dimensions of security culture in Insurance.

[1] https://www.eiopa.europa.eu/media/feature-article/cyber-risks-what-impact-insurance-industry_en

[2] https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack

[3] Perry Carpenter, *"Transformational Security Awareness - What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors"*, USA, Wiley, 2019, p. 85

Legal

72

1,673

20

Law firms continue to be a favorite target of cybercriminals. An October 2021 American Bar Association report found "29% of law firms reported a security breach, with more than 1 in 5 saying they weren't sure if there had ever been a breach and 36% reporting past malware infections in their systems."[1] With an overall security score of 72, law firms hold significant amounts of confidential and sensitive information available now online compared to law firms of the past which relied on physical copies. Law firms are also fighting a double-edged sword: not only does the firm suffer monetary and reputational damages when compromised, but they could also face significant fines for failure to follow government regulations.

The highest dimensions in the Legal sector are Communication (78), Compliance (74) and Attitude (74). Law firms excel at communicating and leverage that critical skill to ensure the entire firm understands and has access to what they need. Employees are well versed in policies and believe it is their responsibility to ensure the organization is well protected.

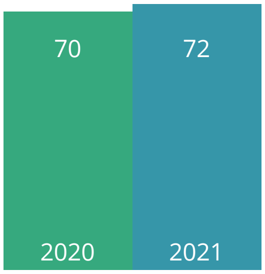


Figure 62: Security culture trends in Legal.

Areas for Improvement

The two lowest dimensions are Behaviors (67) and Norms (69), both of which are Mediocre on the Security Culture Index. The dimension of Behaviors had a three point drop from last year, which may be attributed to pandemic required remote work environments. Again, employees may fully understand and comply with policies, but they need to know how to translate that into action. As with last year's findings, it is important to note the correlation between Behaviors and Norms; an increased focus on reinforcing Norms to drive desired Behaviors, particularly in the current remote work environment, is recommended.

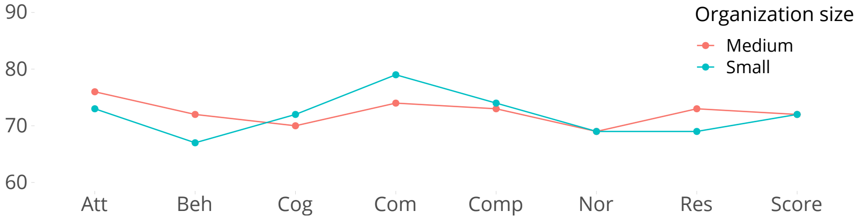


Figure 63: Security culture in Legal according to organizational size.

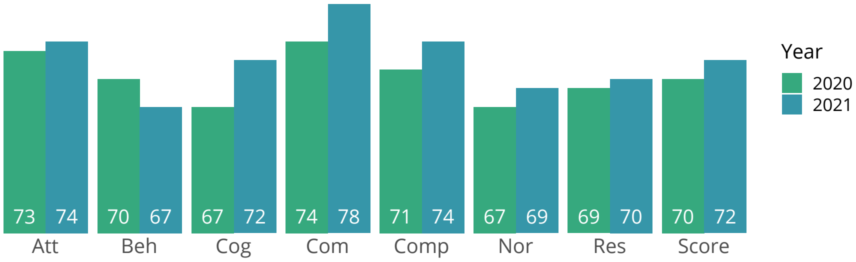


Figure 64: Trends as seen across the dimensions of security culture in Legal.

[1] https://www.americanbar.org/groups/law_practice/publications/techreport/2020/cybersecurity/

Manufacturing

The pandemic-fueled rapid evolution of digital technology to support supply chain operations introduced greater vulnerabilities across the Manufacturing sector. According to the Department of Homeland Security, a "direct attack on, or disruption of certain elements of the manufacturing industry could disrupt essential functions at the national level and across multiple critical infrastructure sectors."[1] Global supply chains are investing heavily in software to better ensure the availability of reliable data for "lean" or "just in time" manufacturing practices which have fallen under scrutiny for COVID-related shortages. Stakeholders must ensure their workforce is provided with the digital skills and security culture mindset necessary to match the industry's increasingly on-demand environment. Again, these rapidly evolving factors are attributed to the Manufacturing sector's low-Moderate score of 71 for the third year in a row.

The Manufacturing sector experienced a notable two point increase in both Behavior and Norms over last year's research as employees have adapted to some changes within the industry. The Communication dimension remained consistent (74) and remains the strongest dimension in the industry for the third year in a row.

71

32,853

119

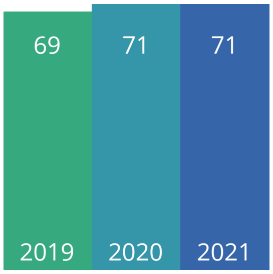


Figure 65: Security culture trends in Manufacturing.

Areas for Improvement

Although better than last year, Cognition remains at a Mediocre rating (68) on the scale, indicating an elevated need for security awareness, as well as an increased understanding of how their cyber hygiene affects the Manufacturing industry's overall security posture. This correlates with the also sub-par rating for Responsibility (69), which indicates a need for increased messaging to employees building their sense of personal responsibility for a stronger security culture.

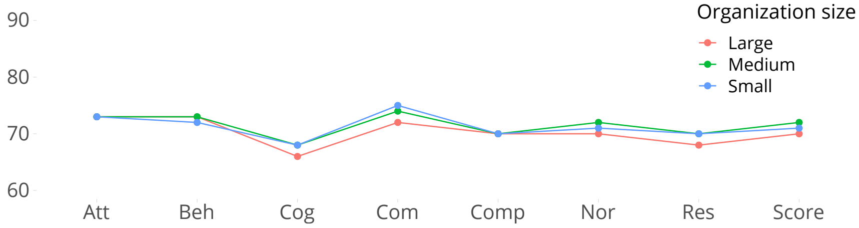


Figure 66: Security culture in Manufacturing according to organizational size.

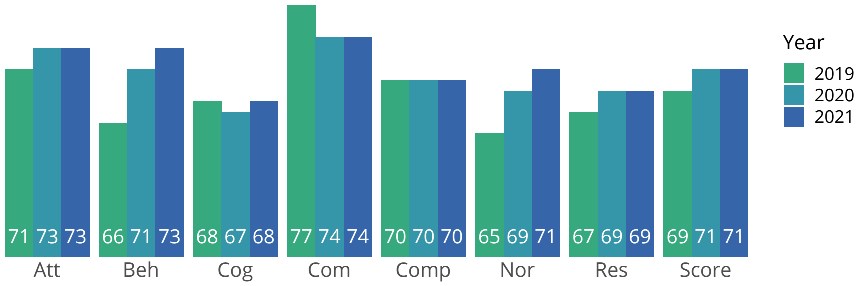


Figure 67: Trends as seen across the dimensions of security culture in Manufacturing.

[1] https://www.cisa.gov/critical-manufacturing-sector

Not-for-Profit

Nonprofits have long been considered an easy target among cybercriminals. With an overall low-Moderate score of 72, Not-for-Profit organizations typically have lean operating budgets focused on marketing campaigns supporting their charter, which results in budgetary restraints on IT operations. As a result, cybersecurity is often neglected.

Communication remains the highest dimension for Not-for-Profits (76), followed by Attitude (74).

Since communicating is a critical component of building a strong security culture, it is important that Not-for-Profits push security information to the right audiences at the right time, both internal and external, raising employee readiness while increasing donor long-term trust and confidence.

Areas for Improvement

The lowest dimension in the Not-for-Profit sector is Responsibility (69) followed by Cognition (70). Not-for-Profits focus on acquiring funds and/or material items to improve the quality of life for a target population. These organizations tend not to have investment dollars to put into securing their digital environments.

Therefore, personnel and volunteers have varied levels of security awareness and best practices. Not-for-Profits will benefit from leveraging low cost or free security tools that are developed for their specific needs, reducing IT operational costs as a barrier.

72

10,509

74

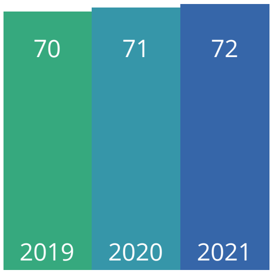


Figure 68: Security culture trends in Not-for-Profit.

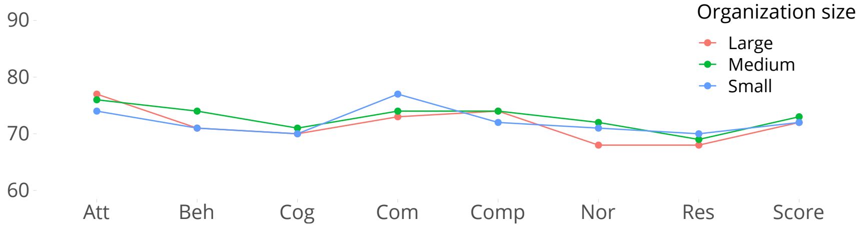


Figure 69: Security culture in Not-for-Profit according to organizational size.

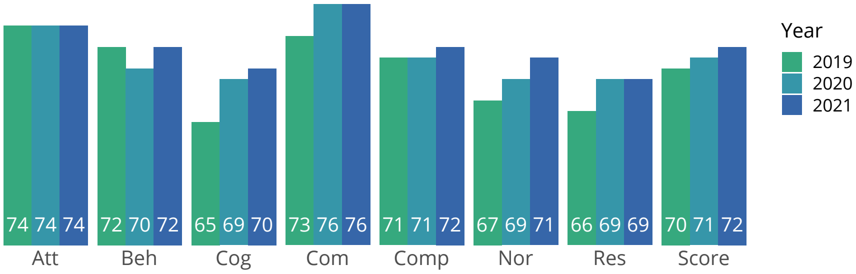


Figure 70: Trends as seen across the dimensions of security culture in Not-for-Profit.

Retail and Wholesale

71

25,776

73

The Retail and Wholesale sector has various compliance requirements ranging from PCI, SOX and HIPAA to various state privacy regulations, yet they remain an attractive focus for cybercriminals. Targets ranging from vulnerable Point of Sale (POS) systems to malicious software (malware) attacks via supply chain vendors (who often have trusted access to the corporate network) provide cybercriminals troves of user and credit card data. Social media and digital payment technologies also provide a host of new challenges. Whether it is social media-enabled social engineering approaches or the implementation of digital wallets (often in support of contact-free payments) and cryptocurrencies, the attack surface continues to expand for this sector. This underscores the need for ongoing investment in information security and employee training. The Retail and Wholesale sector scored one point over last year (71), indicating a continued need for improving the industry's security mindset.

The dimensions Behavior (73) and Norms (71) enjoyed the strongest gains in this year's survey, both increasing by two points. These organizations had to adapt faster because of the "keeping the doors open" effect for retail, yet straddling hybrid environments for office/support functions. Attitude (73) gained only slightly while both Communication (75) and Compliance (71) remained consistent with last year's findings.

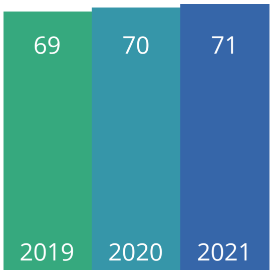


Figure 71: Security culture trends in Retail and Wholesale.

Areas for Improvement

Responsibility dropped one point (68) remaining at a Mediocre rating, indicating that a strong emphasis—reinforced through a variety of communications channels—is needed for employees in the Retail and Wholesale sector to personalize the need for an improved security culture. The Cognition score improved two points (68), but also remains a Mediocre rating, underscoring the need to engage employees with relevant security awareness training.

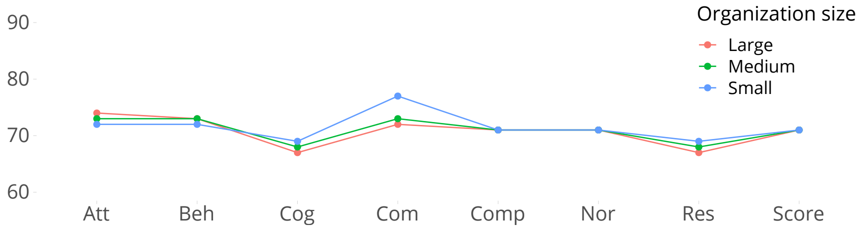


Figure 72: Security culture in Retail and Wholesale according to organizational size.

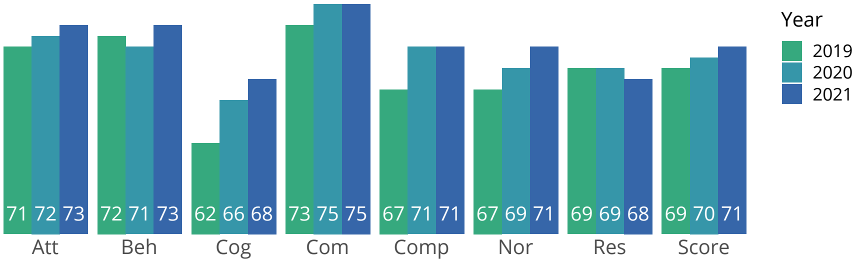


Figure 73: Trends as seen across the dimensions of security culture in Retail and Wholesale.

Technology

76

35,008

214

The COVID-19 pandemic created massive—and likely permanent—changes in the Technology sector. Throughout 2021, COVID-19 variants hindered return-to-office plans, forcing the industry to reconsider their company policies and work cultures in the face of partial or full-time permanent remote work. In addition, these changes led to major technology and human capital investments to allow workers to securely connect and collaborate from anywhere. The distributed, virtual nature of this "new normal" in business operations requires companies to reconsider their approach to security culture. In-person training tools such as posters and fliers have given way to accelerated simulated social engineering testing and online gamification of security awareness training. This industry is particularly accustomed to rapid adjustments as exhibited in their return to the pre-pandemic overall score of 76.

Technology, as expected given their area of expertise, enjoys some of the strongest scores in this survey. Three dimensions improved over last year's results. Norms enjoyed the greatest increase, three points over last year (77). 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. Communication (79) and Compliance (74) increased by one point, while Behavior (77) and Cognition (74) were consistent with last year's survey findings.

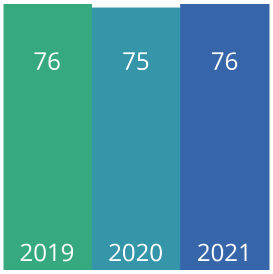


Figure 74: Security culture trends in Technology.

Areas for Improvement

The Responsibility dimension remains in decline for the third consecutive year at 72 while Attitude dropped one point to a still respectable 77. The ongoing downturn of the Responsibility dimension suggests a diverse messaging campaign to employees regarding the professional and personal benefits that a stronger security culture can bring could be in order. The slight drop in the Attitude dimension is likely related to the dramatic increase of ransomware and other headline worthy cyber attacks.

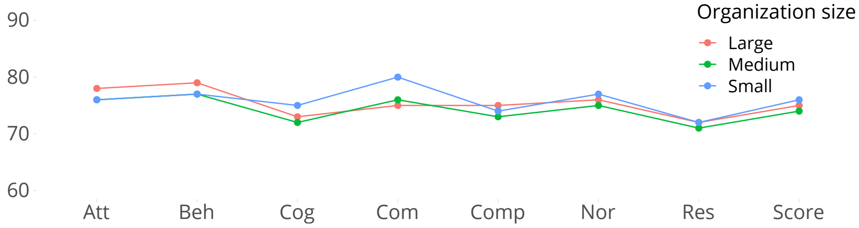


Figure 75: Security culture in Technology according to organizational size.

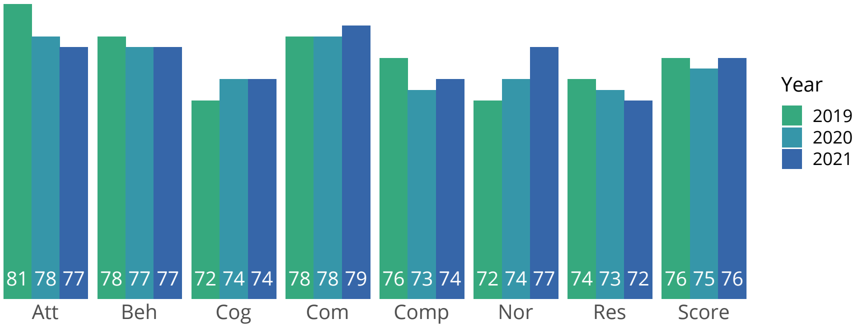


Figure 76: Trends as seen across the dimensions of security culture in Technology.

Transportation

72

The Transportation industry faces a number of logistical and technological challenges. Increased fuel costs, supply chain issues, carrier capacity, staffing and other industry demands have all weighed heavily upon the sector. Transportation encompasses several subsectors to include aviation, mass transit, maritime, rail, etc. that at times require coordinated efforts between public and private sector partners, each with their own unique characteristics and cultural landscape. This diverse landscape requires the need for an effective and sustainable security culture framework that stakeholders can adhere to in an effort to promote a stronger environment. There are many areas of improvement in this year's research results, however, the Transportation industry remains at a moderately low 72.

The industry has exhibited marked improvements over last year's research. Communication (76) is the dominant dimension. Behavior (73) and Norms (72) have improved each by two points. Though Compliance climbed three points to 71, there is still room for improvement. The Transportation industry would be well served building on their strong Communication dimension to generate consensus and cooperative relationships while furthering security culture strategies.

6,867

32

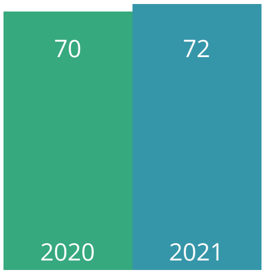


Figure 77: Security culture trends in Transportation.

Areas for Improvement

Although a slight increase over last year, Cognition (68) remains an area that requires additional attention, as well as Responsibility, which remains at 68—both rate Mediocre on the survey. Recently passed legislation[1] could help provide funding necessary to advocate for stronger industry-wide security culture as a critical core business value throughout the Transportation sector.

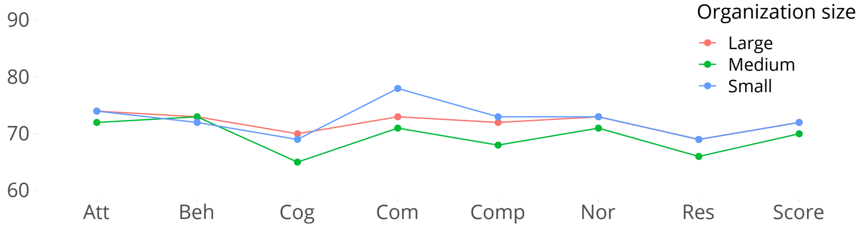


Figure 78: Security culture in Transportation according to organizational size.

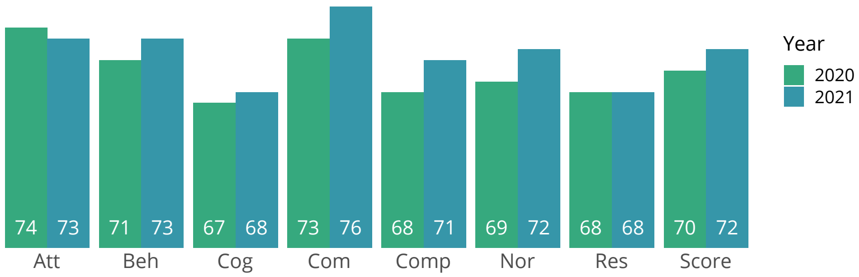


Figure 79: Trends as seen across the dimensions of security culture in Transportation.

[1] https://www.congress.gov/bill/117th-congress/house-bill/3684/text

The Security Culture Survey,
and therefore this report, is created as a
multi-level statistical analytics tool,
where individual respondents are aggregated
to the level of an organization.

About the Report

This report was created by KnowBe4 Research using the highest research standards. The report leverages anonymized data from KnowBe4's Security Culture Survey. The sample size represents 2,910 surveyed organizations around the world, with more than 530,356 employees across 18 industry sectors, effectively making this the largest report of its kind published to date.

Methodology

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

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

76

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

35,008

Number of organizations
This is the number of organizations in this industry.

214

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. 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 2019 to 2021 and represents customers from around the globe. The data for this report is based on a single data collection time point for each employee and was then anonymized and aggregated. All data analysis was performed in the software environment R (r-project.org).

Data Preprocessing

To ensure validity and reliability, the data was cleaned before any calculations were conducted. A listwise deletion of missing data was conducted, which means that responses with missing values were deleted.

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

Statistical Analyses

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

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

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

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

Data Size

The data consists of 530,356 employees and 2,910 organizations. For the trends analysis, the final sample after data cleaning consisted of 514,575 employees and 2,656 organizations that completed the Security Culture Survey. For the industry benchmarks for 2021, the final sample consisted of 257,546 employees and 1,456 organizations that completed the Security Culture Survey. Data was collected from 68 countries.

Industry Data

Table 19: Frequencies of employees and organizations with complete data per industry.

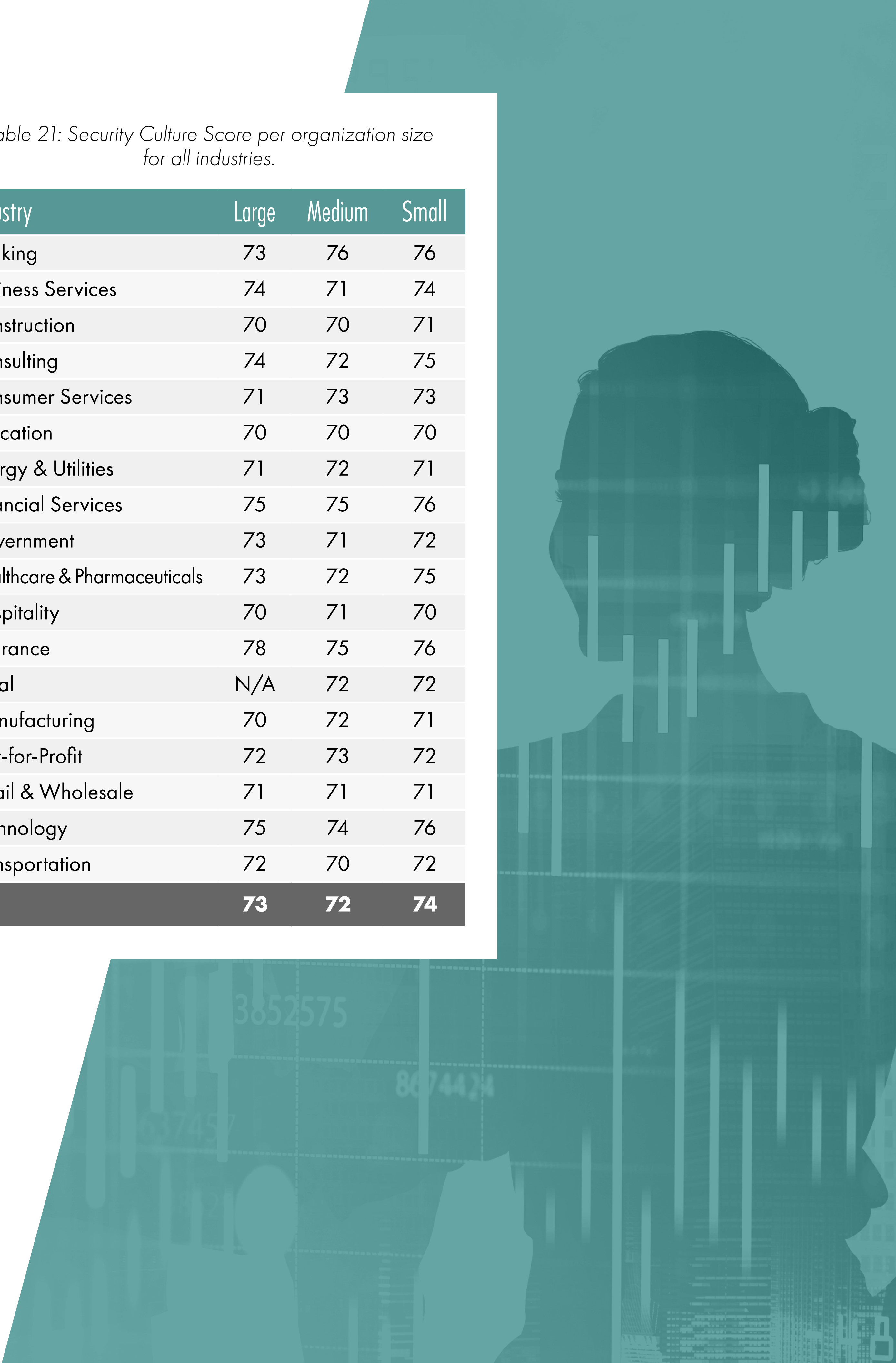
Industry	Employees	Organizations
Banking	14,184	105
Business Services	12,162	102
Construction	4,797	35
Consulting	10,544	55
Consumer Services	3,597	33
Education	9,081	50
Energy & Utilities	10,590	62
Financial Services	26,853	187
Government	20,505	120
Healthcare & Pharmaceuticals	24,761	114
Hospitality	2,233	9
Insurance	5,194	52
Legal	1,673	20
Manufacturing	32,853	119
Not-for-Profit	10,509	74
Retail & Wholesale	25,776	73
Technology	35,008	214
Transportation	6,867	32
Total	**257,187**	**1,456**

Table 20: Descriptive statistics for all industries.

Industry	Max	75%	Median	Mean	25%	Min
Banking	81	78	76	76	75	66
Business Services	84	77	74	74	71	59
Construction	80	73	71	71	68	64
Consulting	85	78	75	75	72	62
Consumer Services	83	75	72	73	69	64
Education	77	73	70	70	68	63
Energy & Utilities	78	73	71	71	69	64
Financial Services	85	78	76	75	73	64
Government	86	74	72	72	69	63
Healthcare & Pharmaceuticals	86	76	73	74	71	67
Hospitality	75	72	71	70	69	63
Insurance	83	77	76	76	73	67
Legal	78	75	72	72	69	62
Manufacturing	80	74	71	71	69	58
Not-for-Profit	81	75	72	72	70	59
Retail & Wholesale	78	74	71	71	69	64
Technology	88	78	76	76	73	62
Transportation	78	75	72	72	69	63
All	**81**	**75**	**73**	**73**	**70**	**63**

Table 21: Security Culture Score per organization size for all industries.

Industry	Large	Medium	Small
Banking	73	76	76
Business Services	74	71	74
Construction	70	70	71
Consulting	74	72	75
Consumer Services	71	73	73
Education	70	70	70
Energy & Utilities	71	72	71
Financial Services	75	75	76
Government	73	71	72
Healthcare & Pharmaceuticals	73	72	75
Hospitality	70	71	70
Insurance	78	75	76
Legal	N/A	72	72
Manufacturing	70	72	71
Not-for-Profit	72	73	72
Retail & Wholesale	71	71	71
Technology	75	74	76
Transportation	72	70	72
All	**73**	**72**	**74**



Regional Data

In this report, we have examined data from the following regions and countries. The table Region is an aggregation of the data up to geographical regions.

Global Overview

Table 24: Global overview – regions.

Region	Score	Employees	Organizations
Africa	72	14,121	52
Asia	73	15,095	39
Europe	73	30,016	141
North America	74	184,701	1,144
Oceania	72	9,635	46
Central and South America	73	2,913	24
All	**73**	**72**	**74**

Global Overview—Small, Medium and Large Enterprises

Table 25: Regions SML.

Region	Small	Medium	Large
Africa	72	71	73
Asia	70	72	70
Europe	73	72	73
North America	74	73	73
Central and South America	74	74	76
Oceania	74	69	67
All	**74**	**72**	**73**

Country Data

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

Table 22: Country data.

Country	Score	Employees	Organizations
Australia	73	7,331	31
Bahrain	70	212	3
Belgium	73	360	7
Belize	69	52	3
Bermuda	77	16	1
Botswana	71	1,403	6
Brazil	72	1,057	4
Bulgaria	79	50	1
Canada	73	7,108	76
Cayman Islands	76	45	1
Chile	71	30	2
Colombia	77	172	1
Costa Rica	83	20	1
Cyprus	84	18	1
Denmark	72	1,005	2
Dominican Republic	76	775	1
Ecuador	75	196	1
Finland	70	15	1
France	67	361	1
Germany	74	197	5
Ghana	74	1,952	1
Gibraltar	79	30	1
Greece	77	79	2
Grenada	70	141	2
Hong Kong	71	1,361	1
India	72	4,972	6
Indonesia	67	62	1
Ireland	78	15	1
Israel	74	282	1
Italy	77	150	1
Jamaica	66	15	1
Japan	76	2,870	3
Jersey	78	117	1
Kenya	75	13	1
Kuwait	75	177	3
Latvia	66	95	1
Lesotho	72	245	2
Lithuania	72	71	1
Malaysia	66	720	3
Malta	75	37	1
Mexico	77	273	3
Mozambique	63	42	1
Namibia	71	1,442	1
Netherlands	70	2,891	20
New Zealand	72	2,304	15
Nigeria	69	516	4
Norway	72	341	4
Philippines	77	751	1
Poland	74	253	1
Portugal	64	400	1
Saint Kitts and Nevis	69	16	1
Saudi Arabia	74	895	3
Singapore	68	2,559	10
Sint Maarten (Dutch part)	68	28	1
Slovakia	73	664	1
Slovenia	72	213	1
South Africa	73	7,877	34
Spain	74	311	2
Suriname	67	85	1
Sweden	77	10	1
Switzerland	71	207	5
Trinidad and Tobago	69	20	1
Uganda	75	606	1
United Arab Emirates	73	216	3
United Kingdom	74	22,144	79
United States	74	177,593	1,068
Zimbabwe	73	25	1

States in the USA

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

Table 23: States in the USA.

State	Score	Employees	Organizations
Alabama	73	3,294	16
Alaska	73	12	1
Arizona	76	4,085	11
Arkansas	72	1,187	10
California	75	22,901	87
Colorado	74	2,103	22
Connecticut	74	834	12
Delaware	76	665	3
District of Columbia	71	1,832	6
Florida	75	6,616	64
Georgia	74	5,606	40
Hawaii	71	65	1
Idaho	72	68	1
Illinois	73	8,742	49
Indiana	73	7,293	40
Iowa	72	984	16
Kansas	74	124	4
Kentucky	73	1,350	21
Louisiana	73	3,854	9
Maine	76	315	7
Maryland	76	2,236	25
Massachusetts	75	3,550	24
Michigan	73	10,133	70
Minnesota	73	6,145	31
Mississippi	74	847	10
Missouri	74	2,066	25
Montana	74	752	7
Nebraska	74	600	9
Nevada	76	652	5
New Hampshire	72	3,766	11
New Jersey	75	2,076	18
New Mexico	72	653	5
New York	74	7,325	55
North Carolina	75	3,981	36
North Dakota	75	186	2
Ohio	73	8,592	64
Oklahoma	75	477	9
Oregon	77	1,796	9
Pennsylvania	73	5,839	33
Rhode Island	77	746	6
South Carolina	74	1,757	14
South Dakota	72	1,931	8
Tennessee	72	2,245	16
Texas	74	13,028	57
Utah	75	3,089	10
Vermont	77	91	4
Virginia	74	6,885	28
Washington	74	4,135	15
Wisconsin	72	4,634	30
Wyoming	76	39	2

Provinces in Canada

Table 24: Provinces in Canada.

Province	Score	Employees	Organizations
Alberta	72	1,235	14
British Columbia	73	1,313	12
Manitoba	73	162	5
Newfoundland and Labrador	73	241	1
Ontario	74	3,468	36
Quebec	76	47	1
Saskatchewan	76	572	6
Yukon	64	70	1

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, and managing director of KnowBe4 Research, where he is responsible for security culture research. Prior to founding CLTRe, Roer created the global de-facto standard Security Culture Framework. His groundbreaking research into security culture metrics provides organizations worldwide with deep insights into the human factors that influence risk and security. Roer is an award-winning specialist on security behaviors and security culture as well as a best-selling author. He is the host of the videocast Security Culture TV and an avid blogger. Roer keynotes at events around the world. He belongs to the Norway Chapter of the Cloud Security Alliance.

Dr. Gregor Petrič

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

Anita-Catrin Eriksen

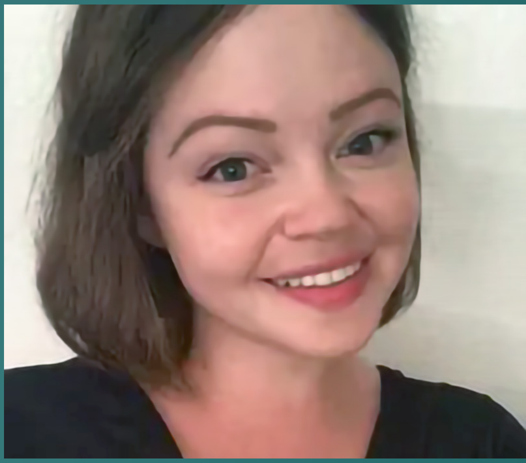
Anita-Catrin Eriksen is a researcher with a social science background who enjoys applying her knowledge and skills to new areas. She loves working with data in programming languages, like R and Python, to produce accessible knowledge and insight. As the security culture researcher at CLTRe, a KnowBe4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

Jacopo Paglia

Jacopo Paglia is a statistician at KnowBe4. His work consists of maintenance of databases, the analysis and interpretation of data, and the creation of reports. Paglia has a Ph.D. in Statistics from the Norwegian University of Science and Technology and a Master of Science (and a Bachelor of Science) in Mathematics from the University of Rome Tor Vergata. He also has experience in software development from both academia and the private sector.

Thea Ulimoen

Thea Ulimoen is a security culture researcher at KnowBe4 Research with over 10 years of hands-on laboratory experience in neuroscience and psychology. She uses her extensive knowledge in these areas to offer unique insights into security culture and human factors in cybersecurity in general. Her academic work in neuroscience has mainly focused on multisensory processing and attention, and she applies this knowledge to interpreting differences in behaviors in response to security threats.



Joanna Huisman

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

Rosa L. Smothers

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

Perry Carpenter

Perry Carpenter (author of, *Transformational Security Awareness: What Neuroscientists, Storytellers, and Marketers Can Teach Us About Driving Secure Behaviors* from Wiley Publishing) currently serves as chief evangelist and strategy officer for KnowBe4. In previous roles, he 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. He holds a Master of Science degree in Information Assurance (MSIA) from Norwich University in Vermont and is a Certified Chief Information Security Officer (C|CISO).

KnowBe4 Research

As the dedicated research arm of KnowBe4, KnowBe4 Research is committed to the creation of world-class research into security awareness, behaviors and culture. By combining and analyzing datasets from the Security Culture Survey with behavior data, knowledge tests and training content consumed by millions of employees, KnowBe4 Research dives deep into how organizations can best reduce their risks. KnowBe4 Research works with billions of data points and uses proven scientific methods to analyze, understand and improve security awareness, behavior and culture.

KnowBe4, Inc.

KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, is used by more than 47,000 organizations around the globe. Founded by IT and data security specialist Stu Sjouwerman, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud and other social engineering tactics through a new-school approach to awareness training on security. Kevin Mitnick, an internationally recognized cybersecurity specialist and KnowBe4's Chief Hacking Officer, helped design the KnowBe4 training based on his well-documented social engineering tactics. Tens of thousands of organizations rely on KnowBe4 to mobilize their end users as the last line of defense.

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

01C04K01