KnowBe4
Research

SECURITY CULTURE REPORT 2024

Anna Collard
Megan Colbert
Joanna Huisman
Dr. Martin J. Kraemer
Erich Kron
Javvad Malik
Miha Matjašič
Rosa L. Smothers

Table of Contents

Introduction

Human factors are crucial to the integrity of an organization's cybersecurity framework. As highlighted by **Verizon's 2023 Data Breach Investigations Report**, a vast majority—74%—of data breaches stem from manipulative social engineering techniques and human error or oversight. As organizations fortify their technical cybersecurity defenses, adversaries rapidly adapt, opting for simpler methods of system infiltration. Cybercriminals tend to bypass the daunting task of breaching advanced technological security measures and instead focus on targeting human susceptibilities.

Consequently, employees have emerged as the preferred target for these adversaries. This positions your workforce as either your most critical defense layer, or your weakest link...you choose. The collective knowledge, attitudes and conduct of employees significantly determine an organization's susceptibility to cyber threats. Therefore, it is imperative to cultivate a strong security culture within the workplace. Employees are at the heart of an organization's operations and can transform into a formidable human firewall, but only if an organization invests in empowering them to recognize and respond to cyber attacks.

The KnowBe4 Security Culture Report

The Security Culture Report is a comprehensive yearly publication crafted by the premier organization in security culture research, KnowBe4 Research. This document stands out as the most in-depth and comprehensive analysis available, offering survey findings from thousands of organizations across the globe and a rich five-year comparative perspective.

This report represents a treasure trove of data-driven insights, brought to life with easy-to-understand graphics. It dives deep into how security measures really affect organizations and the way people act and feel at work. It's become the go-to guide for understanding the true power of a strong security culture. With its broad coverage, there's nothing else quite like it out there.

18 Industries, 6 Continents, 111 Countries

Additionally, the report presents an intricate and exhaustive examination of 18 industries, assessing each one's security culture readiness. It does not stop at industry-specific evaluations but extends to furnish regional insights that encompass North America, South America, Europe, Africa, Asia, Oceania and an additional noteworthy global overview.

A robust security infrastructure hinges on a multi-tiered strategy, with its foundation firmly rooted in the human element. It is essential for security culture to evolve into a persistent, ingrained practice that every member of the organization embraces as a standard operating practice. Such a culture must be like second nature—and thoroughly integrated in every layer of the organization.

The 2024 Security Culture Report is the most comprehensive study of security culture available. It stands as a comprehensive tool, equipping yourself with the knowledge and strategies to foster a more security-conscious culture within your organization.

What is Security Culture?

KnowBe4 defines “security culture” as **the ideas, customs and social behaviors that influence an organization’s security**. Security culture is best understood as the collective mindset, practices and norms that shape how an organization approaches and prioritizes security. This encompasses shared knowledge and thinking patterns, ingrained habits of staff and employees’ demonstrated behaviors in any setting where they carry out their professional duties. When referring to the workplace, we apply a broad view of where and how work is conducted and define security in similarly broad terms.

Under this concept, organizations are encouraged to direct their energy toward boosting employee involvement through evaluations and training, refining processes and protocols and adopting technologies that simplify adherence to security best practices.

For those seeking a more comprehensive exploration of security culture and strategic guidance on establishing a robust security culture program, “The Security Culture Playbook, An Exclusive Guide To Reducing Risk and Developing Your Human Defense Layer” authored by Perry Carpenter and Kai Roer, published in 2022 by Wiley, is an excellent resource.

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

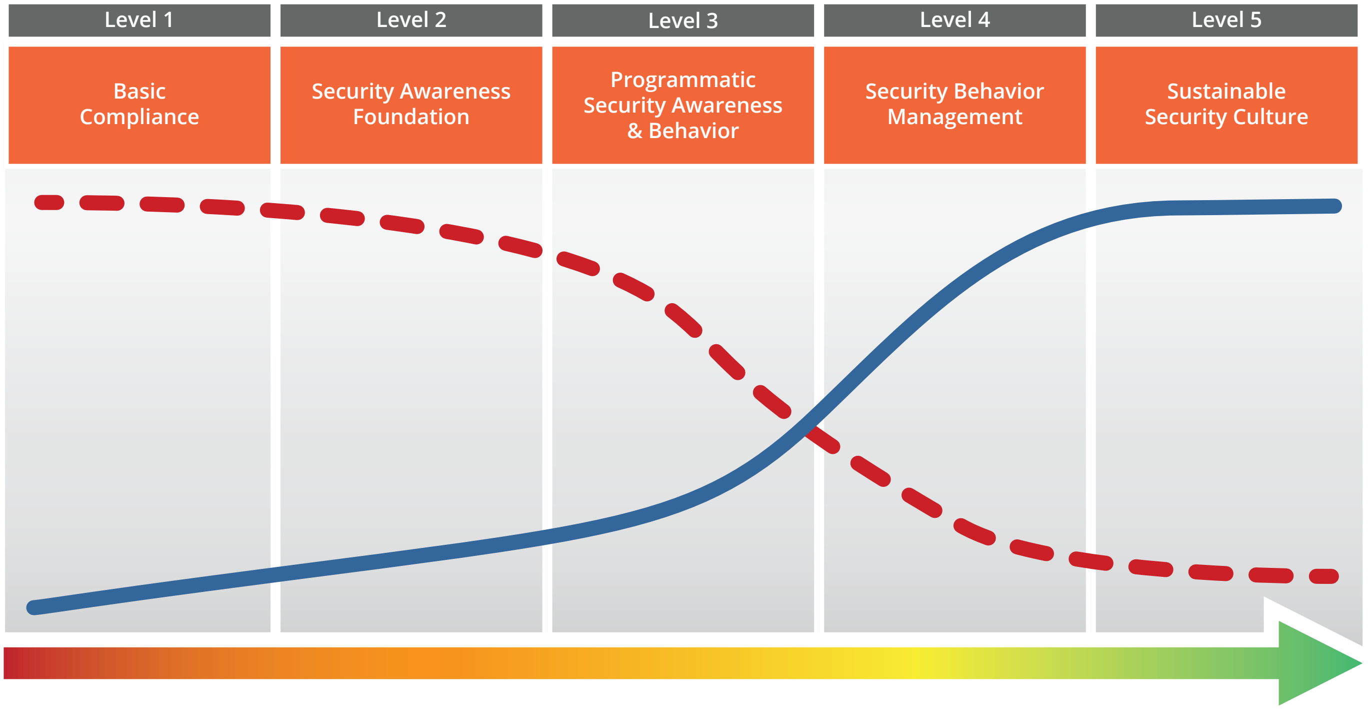
The Security Culture Index (SCI) is the global index for rating organizations based on their security culture score. The index was created by KnowBe4 Research and is calculated by analyzing the security culture of thousands of organizations around the world.

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 KnowBe4 Research team has pioneered the Security Culture Maturity Model, an industry-first tool designed specifically to assess security culture, underpinned by a robust, data-driven and empirical approach. This innovative model draws on the extensive set of security awareness, behavior and culture data collected by KnowBe4, ensuring a comprehensive and insightful evaluation of an organization's security posture.



▬ ▬ ▬ 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

The 5 Maturity Levels

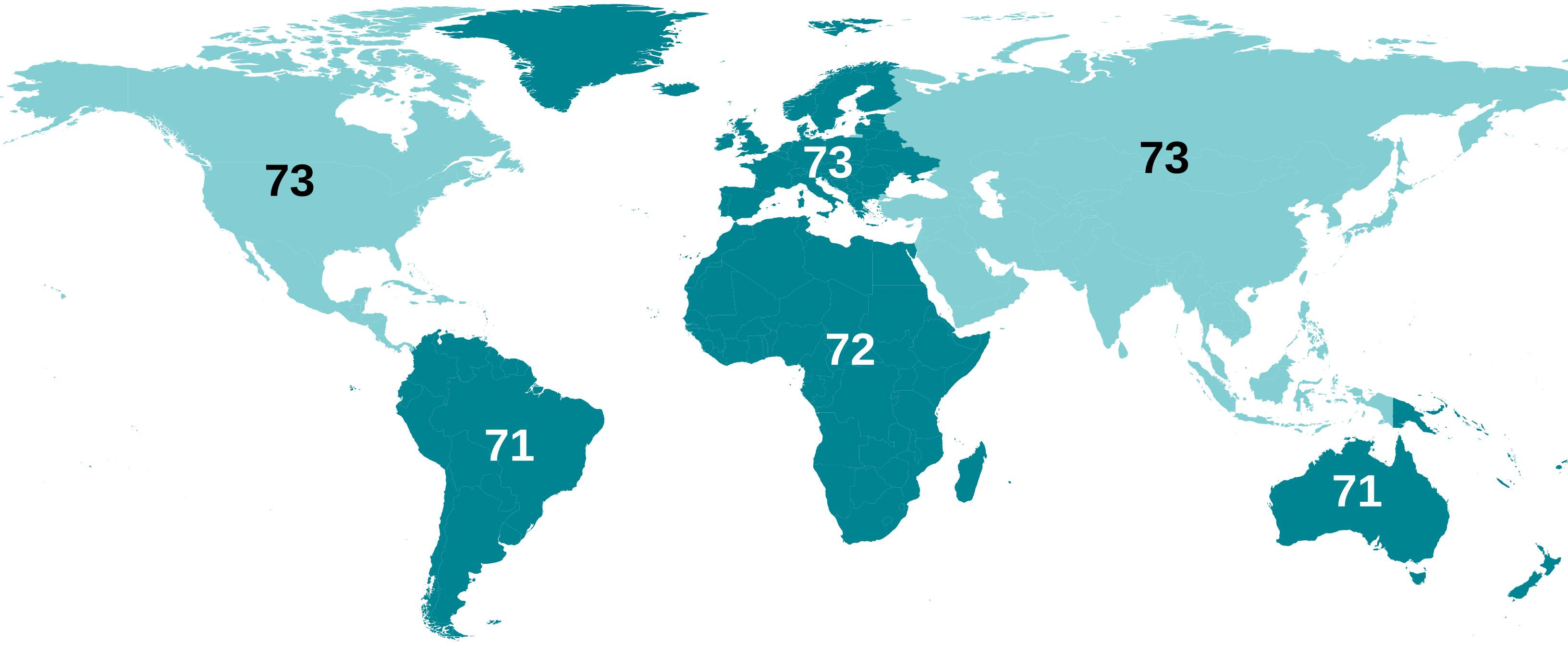
The model describes a spectrum that includes organizations at the most basic level of compliance, where there is little to no conscious strategy for fostering awareness, behavior, or a security-centric culture (Level 1). We then look at organizations with a Sustainable Security Culture (Level 5). These organizations not only meet but exceed standard expectations, and endeavor to influence even the informal norms and social dynamics that shape their employees' attitudes toward security. Read more about these varying 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 guide available for download here: https://www.knowbe4.com/security-culture-maturity-model

Global Overview

By Javvad Malik, Lead Security Awareness Advocate

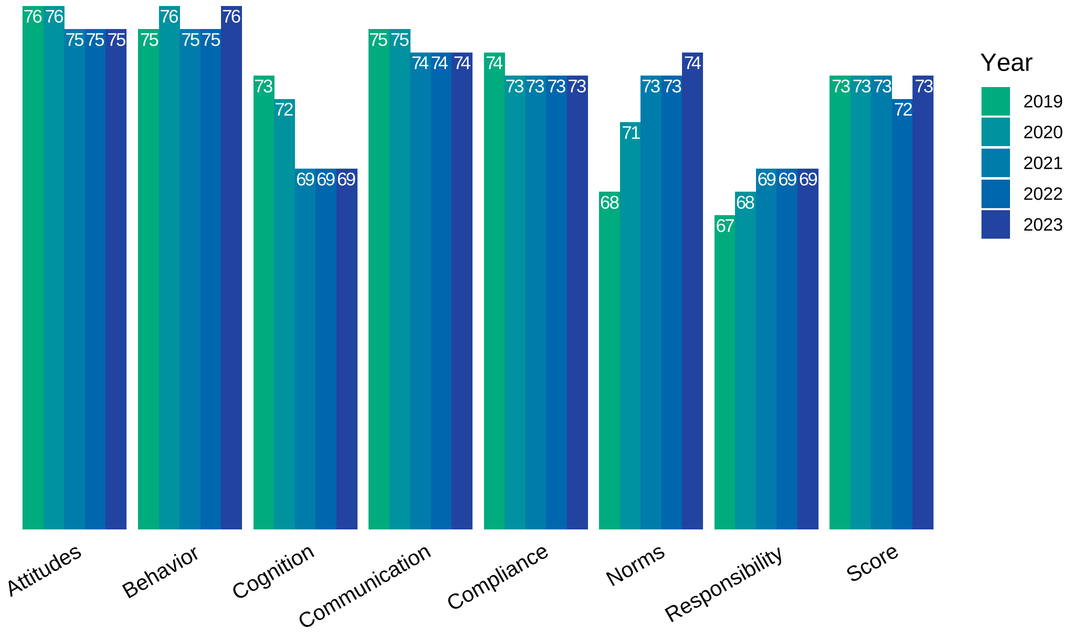


Cultural Adoption

The world may be your oyster, but how does it fare when looking at cybersecurity culture? Approximately 5.35 billion people have internet access, which means 66.2% of the global population are potential targets for criminals. Against this backdrop, strengthening security cultures is more than a corporate challenge. It's a societal imperative.

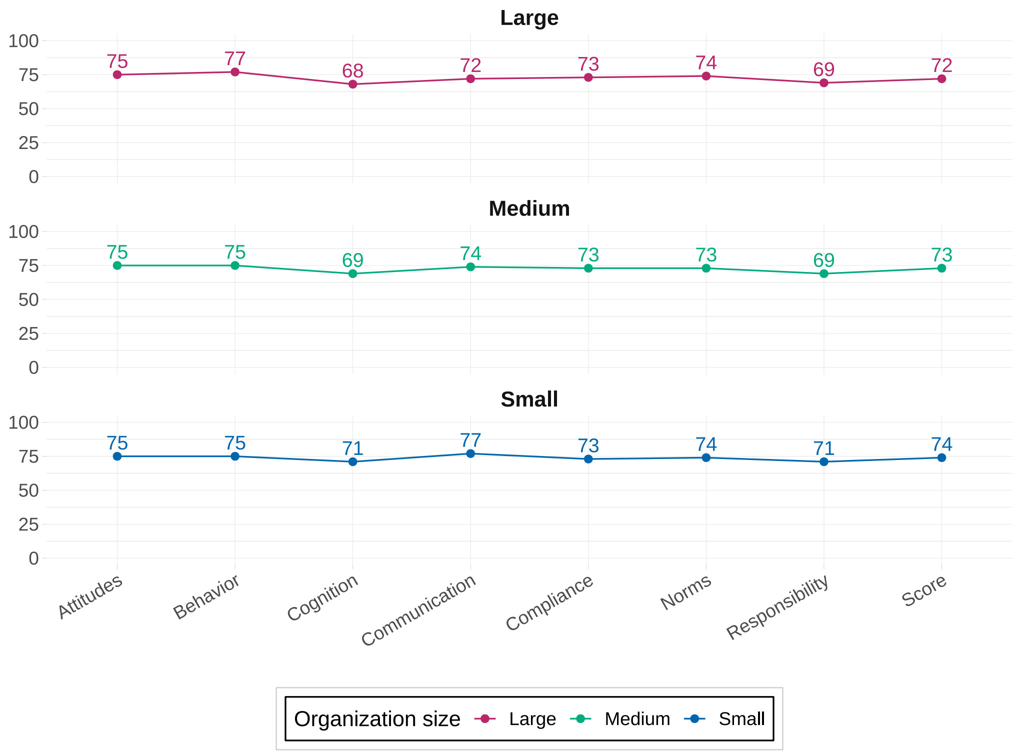
Organizations around the world vary greatly in how deliberate they are in building a strong security culture that aligns with their risk tolerance and overall culture. While many governments and organizations have attempted to implement some form of cybersecurity strategy, their efforts have met varying degrees of success.

Security culture trends across all dimensions worldwide



Many organizations approach cybersecurity culture in the same way they approach a technology project. However, what works for computers and networks doesn't translate well when dealing with humans. This can be why practical steps to build a strong culture falter or regress into a compliance exercise. Such faltering mirrors the outdated security awareness and training models of years gone by, when employees were subjected to an annual dose of awareness training.

Security culture as seen by organizational size worldwide



General Attitudes

The maturity levels of security culture vary greatly across the globe. In some areas, individuals are more aware and vigilant of threats at a personal level, but these do not automatically translate to organizations. In other areas, threats are viewed more as an organizational challenge that does not impact individuals personally.

Anecdotally, it appears security culture grows stronger where it is relevant not just to an organization, but to individuals—when it is something they can take home to share with friends and family.

On a positive note, it appears as if more organizations are embedding cybersecurity initiatives beyond technological controls and understanding that people form an important part in creating a strong security culture.

Key Regulatory Requirements (i.e., Legislative)

There are many existing, updated and new regulatory requirements globally that attempt to bring cybersecurity front of mind within organizations. However, many of these fall short by focusing on technological controls, breach notification requirements or basic awareness. While these are fundamental building blocks of a security culture, they alone cannot sufficiently move the needle.

Security Events/Prevalent Issues

There are many issues around the globe impacting organizations when it comes to security culture. Cyber crime remains a priority for many organizations. The focus is largely on issues such as ransomware while ignoring the fact that social engineering remains the most prevalent method of deploying ransomware.

In 2023, these events left a lasting impact. The shifts to remote or hybrid working models required rapid deployment of technology and incurred cyber debt in the process, which negatively impacted many organizations.

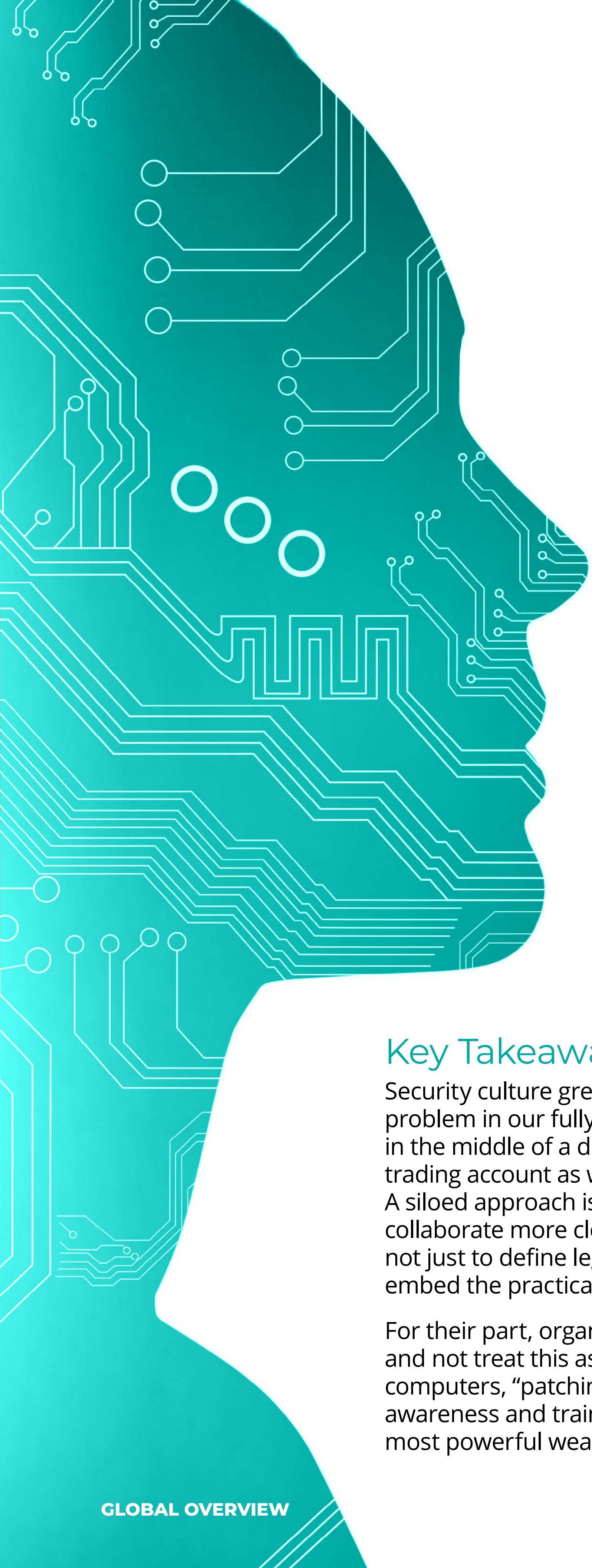
As the COVID-induced panic buying of toilet rolls was starting to wane, global events introduced a new set of complex risks. In 2022, Russia invaded Ukraine, while the following year brought escalating conflict in the Middle East. These are significant because we've seen how cybersecurity has played a prominent role not only among those directly involved in such conflicts but also among supporters from afar.

Dimensions

In 2023, we collected insights on 816,733 employees representing 4,078 organizations. The overall security culture score globally stands at 72 (low moderate), unchanged from the prior year. As one would expect, smaller organizations tend to have higher culture scores. It's far easier to change the culture of a smaller group than a larger one. In fact, Behaviors was the only dimension in which large organizations scored higher than others.

Globally there seems to be less understanding, knowledge and awareness of security, as well as less responsibility.

While there is a great deal of variance depending on geographical location, organization size and industry, the sobering fact is that there is much work still to be done in order to raise the standard in culture.



AI Influences

Of all new technologies, artificial intelligence (AI) will probably have some of the most profound cybersecurity impacts on organizations and individuals. AI is already being used to facilitate disinformation and misinformation campaigns, enhance social engineering attacks, and automate multi-layered and multi-faceted attacks at scale—even by attackers with little technical know-how.

In the coming months and years, as elections, wars and other notable events occur, AI will emerge as an increasingly important tool in the arsenal of criminals. With low awareness and a lack of effective regulation, by the time governments and regulators agree on a way forward, it could be too late.

Key Takeaways

Security culture greatly varies across the world. That's a problem in our fully connected world, where a mobile phone in the middle of a desert can interact with a stock market trading account as well as a banker in an office on Wall Street. A siloed approach is not sustainable. Governments need to collaborate more closely with each other and with regulators not just to define legislation, but also to demonstrate and embed the practical steps needed to build a strong culture.

For their part, organizations need to look at the human challenge and not treat this as a technological issue. Unlike patching computers, "patching" humans requires a sustained effort of awareness and training. To quote Nelson Mandela, "Education is the most powerful weapon which you can use to change the world."

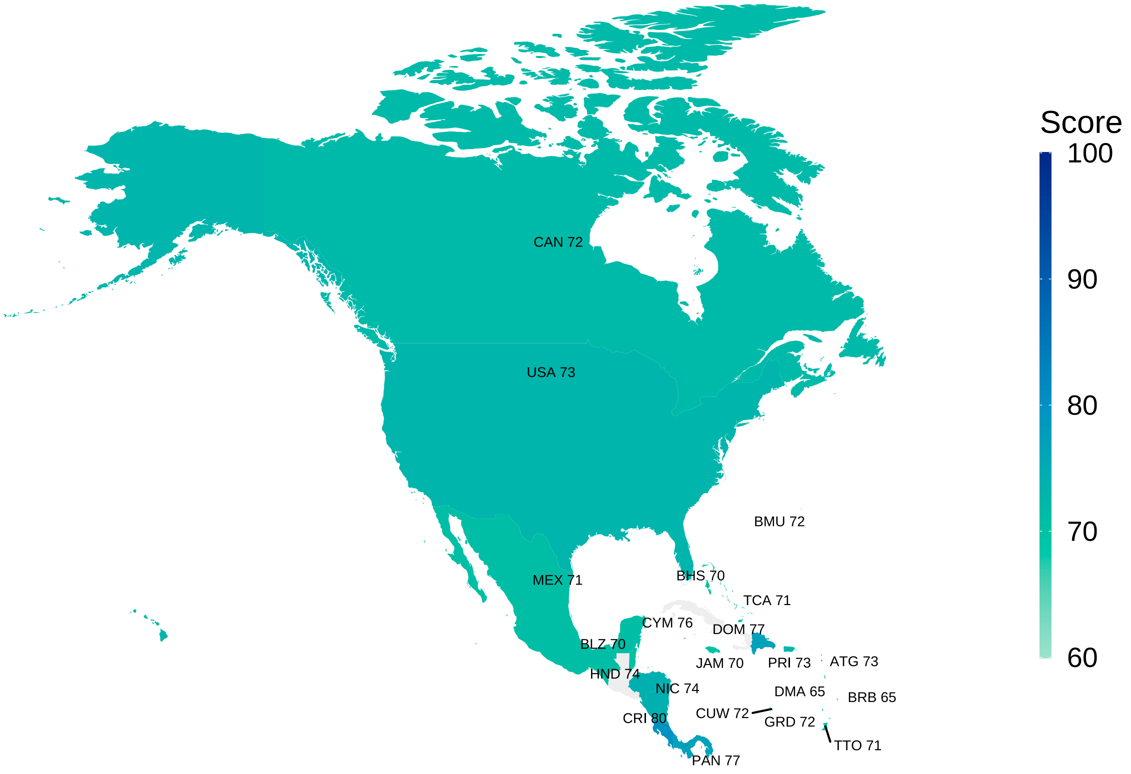
North America

By Erich Kron, Security Awareness Advocate

Cultural Adoption

The importance of security culture is gaining momentum in North American organizations, especially among leaders. The North American Manufacturing sector has sustained a decades-long emphasis on security culture, and organizations across industries have observed the fruits of this labor: safer working environments and fewer accidents. North American leaders understand how a strong culture can have similar positive impacts on cybersecurity. Many of the organizations that have successfully built a strong safety culture are applying the same strategy and tactics to improve their security culture.

Security culture in North America



Alongside cultural awareness, supply chain, vendor management, and all other types of third-party risk have become a hot topic. As such, smaller organizations supplying goods and/or services to large organizations must address their own security culture or risk losing large contracts. For organizations operating in countries that require strong physical security, the need for cybersecurity is more of an evolution than a new idea.

General Attitudes

Organizations across North America are realizing that cybersecurity is a critical part of business. They recognize that employees aren't the weakest link; rather, they are a key defense against these attacks. For their part, employees are realizing that while they are not expected to be cybersecurity experts, they do have a significant role in the organization's cybersecurity readiness. Employees are learning that cyber attacks do not cease to be a threat when they head home for the day. Cyber risks are becoming a part of people's personal lives, as well. As a result, they often become much more receptive to education and learning habits that can protect them personally.

The KnowBe4 survey found that organizations that deal with money are top performers in the security culture game. This makes sense given the stakes. Organizations in the Insurance, Financial Services and Banking industry have been targets of traditional and cyber crime for decades, so a higher level of security culture is not unexpected. Unfortunately, the Education industry comes in last with a score of 69, eight points off the leaders. This industry is often understaffed, with funding being a major hindrance. This translates into tired, hurried people, a favored target for cybercriminals. These U.S. security culture scores are similar to those across the rest of North America (Canada and Mexico).

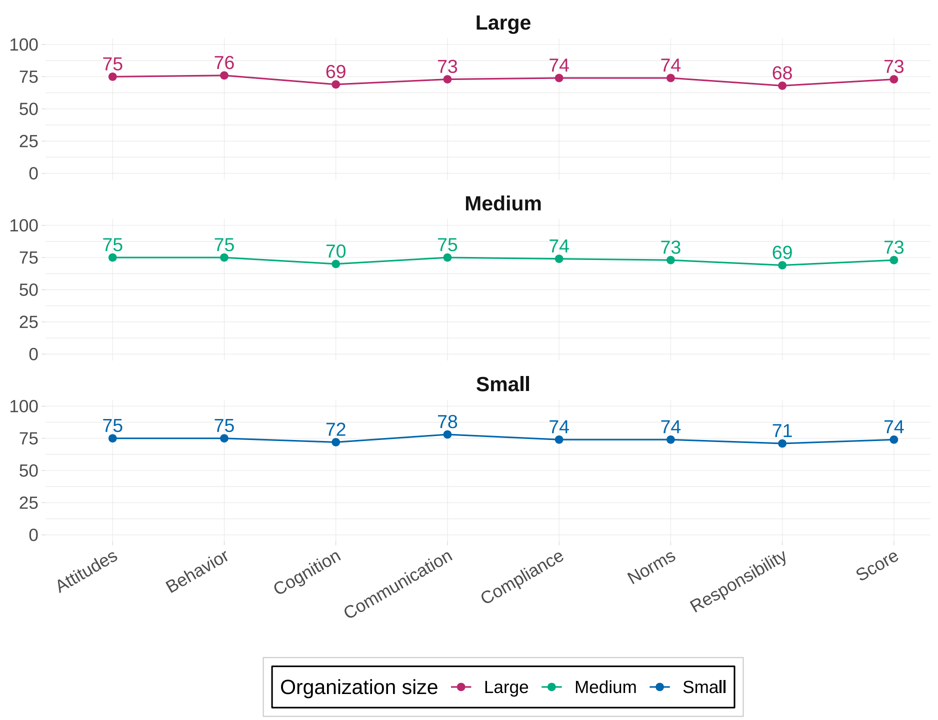
Key Regulatory Requirements (i.e., Legislative)

While there are a number of significant data privacy and security regulations that can impact organizations in North America, one of the more significant is related to a recent Securities and Exchange Commission (SEC) requirement that publicly traded companies report a material cybersecurity incident within four business days of materiality determination.

Security Events/ Prevalent Issues

Ransomware continues to be the hot topic for both executives and security practitioners due to the resulting damages and other impacts, which are often transparent to the general public. Some top new stories highlighted Caesars Entertainment, MGM Resorts and Clorox as targets of the same ransomware group, with losses in the hundreds of millions of dollars and countless hours of downtime.

Security culture as seen by organizational size in North America



Dimensions

As with industry comparisons, survey data for the U.S. versus North America as a whole are quite similar, with small organizations beating out the larger ones in overall score. It's not surprising to see that large organizations may lag in some dimensions. A key part of establishing a good security culture is communication from leadership, something that tends to be much easier for small organizations. In addition, with fewer people on staff, it makes sense that employees of smaller organizations may feel more responsibility for security. For them, it's just another of many hats they wear as part of a small company. Among the regions evaluated in the report, North America, which represents the highest number of employees/ organizations surveyed, experienced a slight decline in overall security culture score, falling one point to 73 (low moderate).

Language Localization

Language localization is very important when working to influence security culture. While some people confuse localization with translation, the two are very different when it comes to impacting culture. Using locally relevant phrases or situations aids understanding much more than simply changing a word or phrase from English to another language. This nuance can also be important when communicating with employees who speak the same language but in different parts of the world. U.S. English, Canadian English and UK English may seem similar but can be miles (or meters) apart when it comes to making a point resonate with an audience.

AI Influences

There is no question that AI is a hot topic, but it does not represent a completely new attack vector. Much like a certain search engine fundamentally changed the way we use the internet by making things more efficient, AI will do the same for cyber crime. It will help attackers scale up attack volumes; it will dramatically improve translations; and AI-generated deepfakes will become a valuable tool. Even so, attacks will continue to follow the same core formula. Attackers will use phishing to elicit emotional responses, and scared victims will make mistakes by wiring money or introducing malware into systems. Ultimately, defense will be the same—that is, watch for the usual signs of a social engineering ploy.

Key Takeaways

Security culture discussions have hit the boardroom, and organizations are understanding the importance of the human factor in a successful security program. Vendors are being scrutinized more than ever and are expected to have a strong security culture themselves—simply because it is too risky to do business with soft targets for cybercriminals.

Financial organizations and those that handle large sums of money continue to lead the charge simply because the stakes are so high. Unfortunately, Government, Manufacturing and Education represented some of the lowest scores despite being some of the biggest targets, including for ransomware. In those industries, it's crucial to spend money and other resources very wisely simply due to their scarcity.

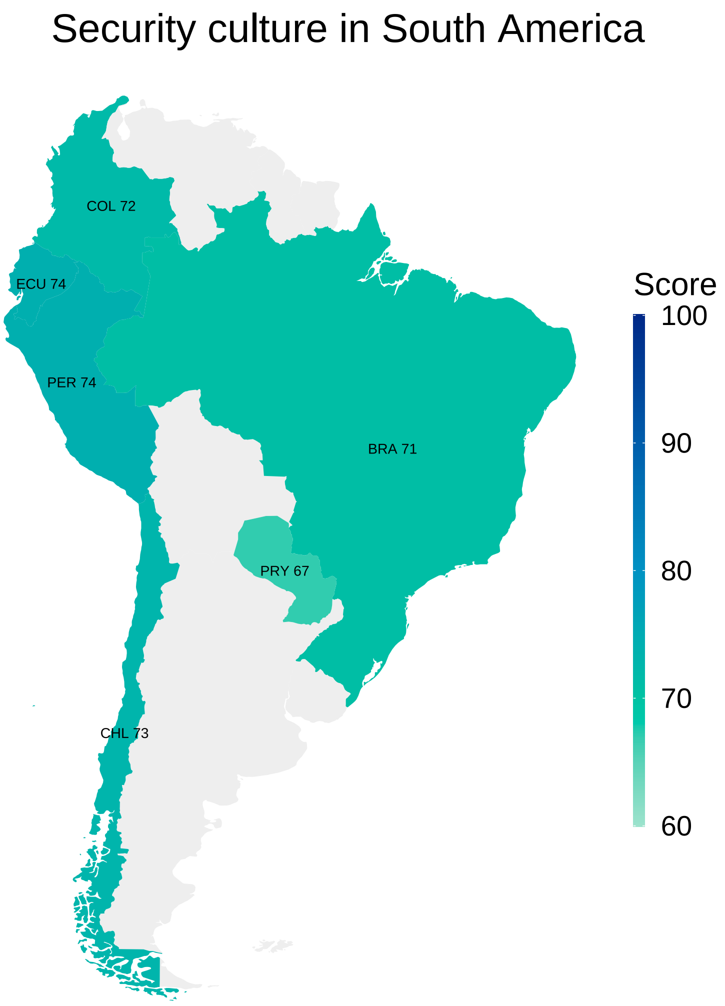
South America

By Joanna Huisman, Senior Vice President of Strategic Insights and Research

Cultural Adoption

Organizations in South America are grappling with the significantly rising challenges of cyber attacks. According to the Council on Foreign Affairs, the region is often neglected for several compelling reasons. To begin with, threat intelligence firms have limited motivation to prioritize South America ahead of more expansive markets. Additionally, cybersecurity domains tend to concentrate on well-known, prominent threat actors, neglecting the rise of nascent ones. Finally, the uneven levels of development throughout the region result in markedly diverse cybersecurity requirements among the various countries.

Moreover, there is a significant communication gap between nations. Influential leaders fail to engage in the necessary dialogues that span borders, leading to systemic unpreparedness within organizations to effectively confront the core issues. This deficiency cascades to the workforce, where employees lack the requisite training to detect, report and prevent attacks. The root of the issue lies in the fact that employees may lack awareness, feel a sense of disconnection from responsibility, or exhibit apathy toward the situation.



To address this issue, organizations must first look at the human factors and adopt comprehensive, continuous training and testing to drive strong cyber hygiene practices across the workforce. This, coupled with robust business continuity plans and proactive prevention strategies, will help shift momentum toward fostering a culture where employees adopt more secure behaviors and take appropriate ownership of cybersecurity.

General Attitudes

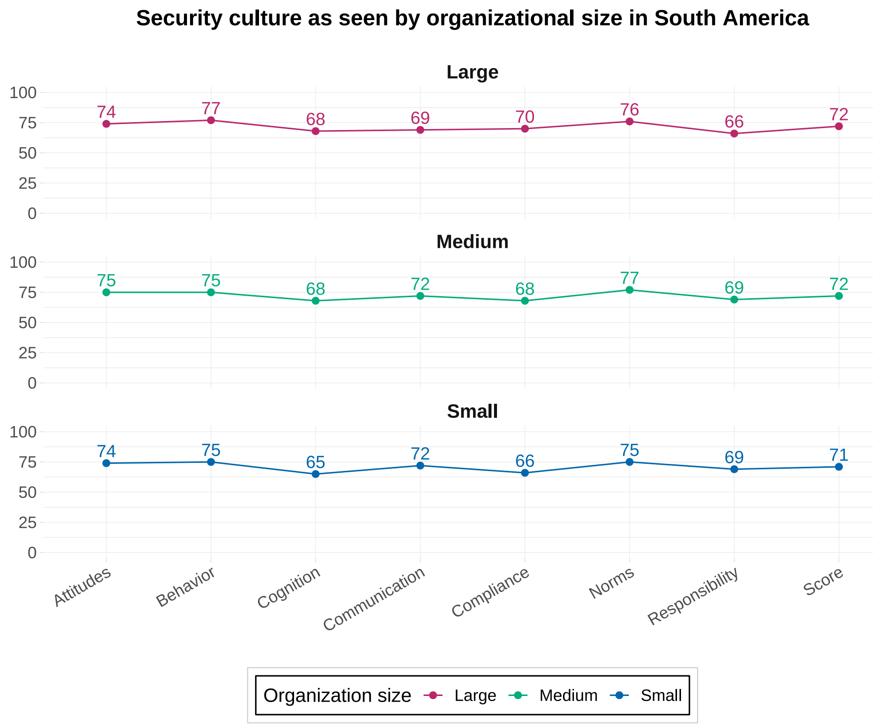
Recent research indicates that cyber attacks are escalating rapidly in South America, with phishing and ransomware emerging as the primary tactics. To combat these threats, security awareness training remains an essential countermeasure. Improving the security culture within South American companies requires a thorough examination of various cultural dimensions to pinpoint specific weaknesses.

By reassessing and refining their strategies accordingly, organizations can foster a more robust security culture. This heightened state of preparedness—where employees are well-informed and the company actively promotes and disseminates knowledge—can have a positive, transformative impact on security culture. Low scores in the Responsibilities dimension underscore a lack of investment in cultivating the human aspect of security, which is crucial for recognizing and responding to social engineering attacks.

Key Regulatory Requirements (i.e., Legislative)

Cybersecurity frameworks across South America display a spectrum of development. Colombia is at the forefront, boasting a robust set of cybersecurity, cyber defense and risk management strategies outlined in the National Council of Economic and Social Policy (CONPES). This policy delineates an incisive scheme for cybersecurity measures designed to bolster digital safety for individuals and the nation, detailing the entities mandated to enforce regulations and manage risks.

Brazil delegates its information security coordination to the Institutional Security Office of the Presidency (GSI). In line with a presidential directive, the GSI played a pivotal role in formulating the National Information Security Policy, which proposes the formulation of quintuple strategic pillars: cybersecurity, cyber defense, the safeguarding of critical infrastructure, the security of classified information and the prevention of data breaches. Argentina puts a premium on data privacy, championed by its Personal Data Protection Law. This law is stringently executed by the Data Protection Authority (DPA) and has garnered recognition from the European Commission for its parity with established international privacy regulations, such as the GDPR. Chile's cybersecurity policy for 2023-28 sets its sights on creating a resilient digital framework that prioritizes user rights, cultivates a security-conscious culture, and fosters both national and international collaboration. This policy further aims to stimulate the cybersecurity industry and scientific inquiry within the field.



Security Events/Prevalent Issues

According to Infosecurity Magazine, in 2023 South America stood out as one of two regions that did not witness a decline in data breaches, with incidents impacting over two million accounts. (The other, Antarctica, is not included in this assessment.) Notably, in September of the same year, Colombia suffered a significant cyber onslaught targeting numerous websites. It was one of the largest against its digital infrastructure and indeed within South America in recent memory.

Dimensions

For South America, the overall security culture score is categorized as low moderate, standing at 71. We strongly advise entities in these areas to adopt robust security culture practices, which should include both training and evaluative measures. Peru and Ecuador are at the upper end of the spectrum, each securing a mid-moderate tally of 74. Paraguay is on the lower end with a score of 67, indicating a mid-mediocre security culture. Paraguay's assessment reveals a disparity between perception and knowledge; its Cognition score of only 59 demonstrates a considerable gap in understanding security threats. Conversely, the Attitudes score stands at 75, indicating that while employees recognize the importance of security, their grasp of the threats and how to apply their training effectively is lacking.

Peru and Ecuador face similar challenges in the dimensions of Cognition and Responsibilities, suggesting that employees lack essential training and insight into the security concerns and practices pertinent to their industries. This deficiency hinders their ability to integrate security culture into their daily behaviors. In Brazil, home to the most extensive dataset in South America, industries primarily struggle with Responsibilities and Cognition. This suggests that despite acknowledgment of security's significance, there's an overarching issue with assuming accountability and comprehending the threats, hindering the implementation of effective security measures.

It's important to highlight that the sample sizes from various South American countries are small, indicating a general lack of fundamental security measures within numerous organizations. Brazil is notable for having contributed the most substantial sample size in South America.

Language Localization

Given that Spanish and Portuguese are the most widely spoken languages in South America, most training and awareness providers offer a substantial amount of cybersecurity awareness and training content in these languages. This strategy will help make the material relevant and relatable for users, fostering better engagement and learning outcomes.

AI Influences

Efforts to nurture talent are fundamental for a flourishing AI ecosystem in South America, and this is complemented by the development of robust regulatory frameworks that ensure the responsible use and progress of AI. Research suggests that the momentum for AI adoption in the region will be fueled by the overarching imperative for companies to undergo digital transformation. Additionally, the benefits derived from enhanced computational power and increased resilience to unexpected market fluctuations will catalyze this growth. On the public sector front, AI presents an unprecedented opportunity for South American governments to address and rectify deep-seated challenges and inefficiencies that have historically impeded the region's social and economic advancement.

Key Takeaways

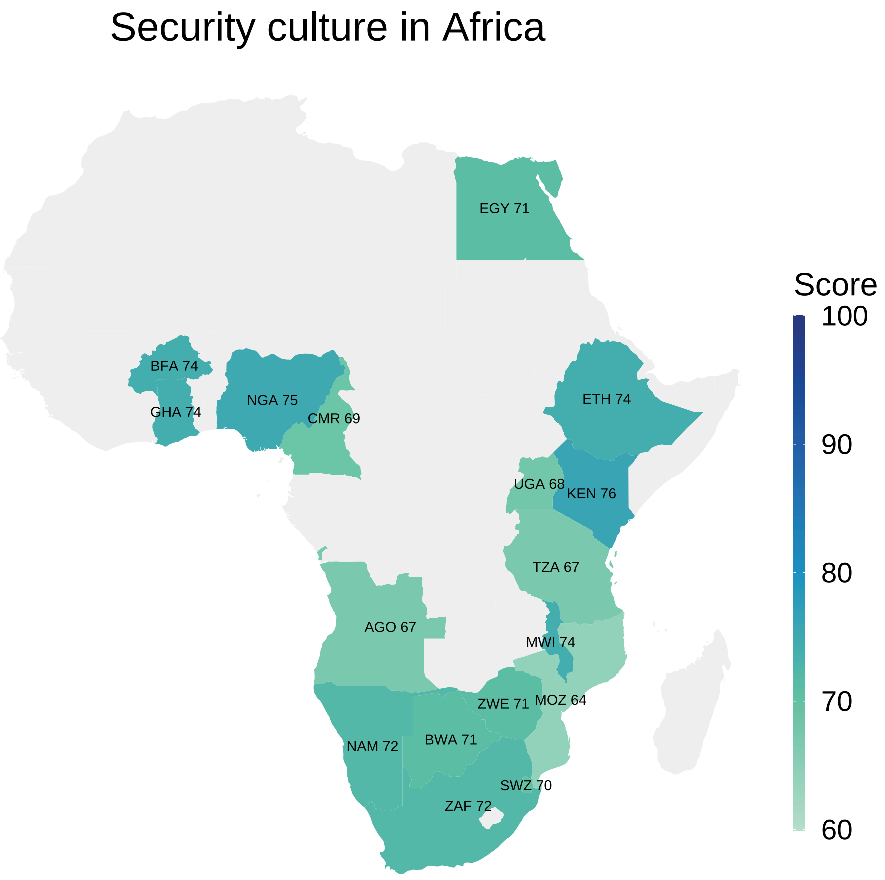
The cybersecurity threat landscape in South America is troubling, and projections indicate a worsening trend. To bolster defenses against the rise of social engineering tactics that have led to unprecedented ransomware attacks, a critical investment in workforce readiness is essential. Businesses must exert stricter diligence in formulating policies and enforcing employee adherence to these guidelines. Furthermore, nations across South America would benefit from improved collaboration on intelligence regarding cyber threats and should actively contribute to a global information-sharing ecosystem. Participation in initiatives such as the Latin American Cybersecurity Research Network is also vital, as it affords deeper insights into evolving threats, as well as access to advanced theories and methodologies in cybersecurity.

Africa

By Anna Collard, Senior Vice President of Content Strategy & Evangelist for KnowBe4 Africa

Cultural Adoption

With a median employee age of 19 years, Africa's share of the global workforce is projected to become the largest in the world by 2100. The United Nations projects that by 2050, Africa's population will reach close to 2.5 billion, meaning that more than 25% of the world's population will be African. Africa is a region of considerable genetic, linguistic, cultural and economic diversity. With anywhere between 1000 and 2000 languages, Africa is home to approximately one-third of the world's languages. In total, there are at least 75 languages in Africa with more than one million speakers. This cultural diversity has an impact on technology and cybersecurity adoption, particularly when content is available only in English. In 2023 we collected insights from 147 organizations across 19 African countries.



General Attitudes

In this region of youth and growth, technology and connectivity usage are rapidly increasing. This digital revolution brings significant potential benefits to economic transformation and job creation, but it also comes with enormous risks and challenges, such as a growing digital divide and increased cyber risks.

Africa has had the most exponential growth in cyber crime over the past few years, particularly among small- and medium-sized organizations. According to Check Point Research, African organizations experienced the highest average number of weekly attacks per organization in the first quarter of 2023. There is a linear relationship between the continent's GDP and cyber crime; as one increases, so does the other.

Key Regulatory Requirements (i.e., Legislative)

In order to address rising cyber crime, some African countries have imposed strict regulatory compliance laws. However, the majority of African countries still lack adequate cybersecurity regulations and enforcement capacities. Currently, only 15 of 55 African countries have ratified the African Union's Convention on Cybersecurity and Personal Data Protection.

Security Events/ Prevalent Issues

African organizations face significant cybersecurity challenges, such as a lack of priority by governments, a relatively low level of general cyber awareness, and a lack of IT and cybersecurity skills. 2023 was a difficult year for Sub-Saharan Africa's economy, with growth slowing to 3.3% from 4% in 2022. The region faces some of the most daunting challenges in the world—including limited resources, urgent humanitarian and development needs, energy crises, poverty and high youth unemployment rates. These challenges may explain a lesser focus on perceived non-business critical tasks such as cybersecurity culture.

Dimensions

The KnowBe4 Security Culture average score is 72 (same as the prior year) for the assessed organizations from 19 countries across Africa. This finding shows a low-moderate level of security culture, which is aligned with the rest of the global regions. However, there are wide varieties by sectors and by countries. For example, the Kenyan banking sector outperformed all other industry sectors on the continent with an average score of 83 (10 points above the average). African banks and the financial industry have a long history of more mature security cultures. They maintain large SOC and CSERT operations and are a major employer for security professionals. Lower-performing culture scores can be seen in the Public, Construction and Education sectors. The Hospitality sector has also scored on the low end in some countries.

The best-performing African countries in this report are Kenya, Nigeria and Ghana, all which have more mature cybersecurity strategies driven by their local governments. In fact, Ghana's cybersecurity success has boosted it from 89th place to 43rd on the 2020 International Telecommunications Union's Global Cybersecurity Index (GCI). It is among just seven African countries in the top 50 GCI globally.

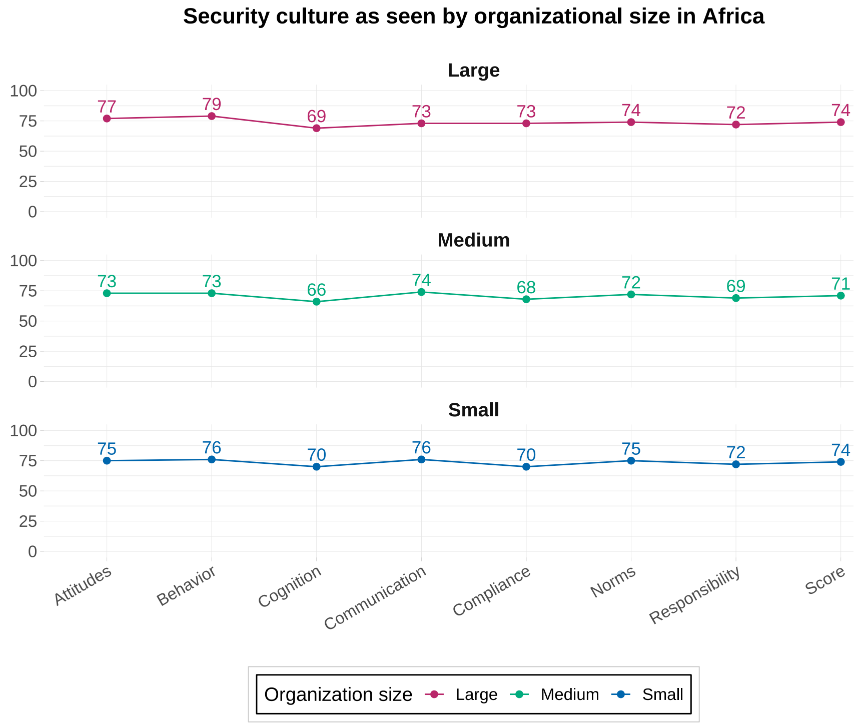
In terms of assessed dimensions, Attitudes, Behaviors, Communication and Norms scored relatively high across all sectors and countries. This could be an indicator of a slight increase in cyber awareness among African employees, driven by corporate security culture programs or an increase in general media coverage. Despite this increased awareness, the low score of Cognition across all sizes shows a lack of real understanding of the threats and impact. We've seen this trend mirrored in our locally driven consumer surveys, as well. People seem to be more concerned about the cyber threat—but lack understanding of what, exactly, they are dealing with or how to protect themselves.

AI Influences

Based on KnowBe4's 2023 surveys on the adoption of AI on the continent, sentiment toward AI and new technologies is highly positive. Nevertheless, African users are concerned about ethical implications, and 90% believe AI tools should be regulated to ensure responsible use.

In another KnowBe4 2023 generative AI survey across South African security leaders, over one-third (36%) of respondents said their organizations don't address or regulate the potential misuse of generative AI within their organization. Just over half (58%) of respondents said no specific training is provided about identifying and countering AI-generated misinformation or deepfakes.

These challenges need to be addressed through a combination of regulation, guidelines and awareness training. Special attention should be given to societal threats posed by malicious use of new technologies, such as deepfakes, especially when used for political manipulation. Major elections coming up in South Africa and other areas of the continent will drive the need for education campaigns. More public-private partnerships are required to assist African people and organizations to build capacity, address the skill shortage, and stay safe in this ever-growing digital world.



Key Takeaways

The South African Council for Scientific and Industrial Research (CSIR) expects an increase in cyber attacks on government departments and critical infrastructure, impacting not just private sector organizations but also societies and national economies.

The majority of African organizations are embracing emerging technologies and embedding them into day-to-day operations. However, not enough is being done yet to regulate use or educate users on risks related to disinformation, security and privacy, as well as ethical concerns, such as bias, inaccuracies and impact on critical thinking.

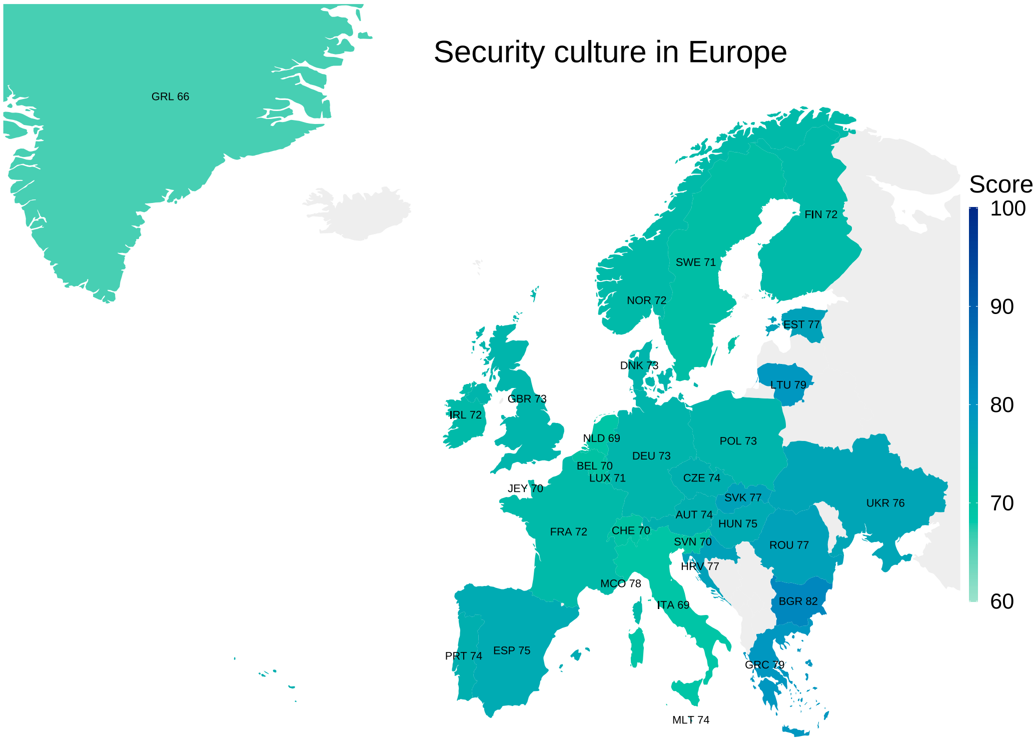
Europe

By Martin J. Kraemer, Security Awareness Advocate

Cultural Adoption

Security culture is understood to varying extents across Europe and its industries. As a concept, it is increasingly being adopted and frequently discussed among security professionals, particularly in sectors with traditionally high levels of digitalization, such as finance, banking and IT. In other industries, security culture is often considered later in the maturity cycle of cybersecurity—slated for attention only after the initial phase of security awareness has been addressed.

While some organizations have a good understanding of security culture as both a process and a strategic measure, many have yet to take their first tactical steps toward achieving that goal. Those that have done so realize that shaping select security behaviors is essential in developing a security culture. These organizations acknowledge that in a proactive security culture, employees have an inherent understanding that secure behavior extends beyond participating in phishing simulations. These employees are intrinsically motivated to add to the security posture of their respective organizations.



However, security culture maturity levels vary greatly across Europe. In some areas, there is little to no recognition for the human element in cybersecurity, necessitating an initial focus on raising awareness. Even though the human factor is still the largest attack vector to any organization, there seems to be a lack of appreciation for that fact—and for the specific attacks that can be launched against individuals.

Europe comprises 44 sovereign countries with a total of 746 million people speaking 287 different languages, 24 of which are recognized as official languages of the European Union.

General Attitudes

For the most part, organizations across Europe understand that people must be part of the defense of any organization to increase its level of resilience. Security awareness is no longer understood as a checkbox exercise for satisfying compliance requirements. It is increasingly seen as a strategic initiative to foster a security mindset in the organization.

Security is often still considered the responsibility of a single team or unit. In organizations that lack an appreciation for and collaboration on cybersecurity across business departments, security professionals struggle to gain traction. This is evidenced by the relatively small number of Business Information Security Officers (BISOs) hired by organizations. The role of the BISO is of strategic significance toward a more secure future as they build the bridge between security and business.

Key Regulatory Requirements (i.e., Legislative)

The EU is a leading force in legislation and regulation, which also drive cybersecurity in the region. Traditionally, legislative efforts are focused on upholding fundamental human rights in times of rapid technological advancements. Like other regions, the EU has also set out to protect businesses from cybersecurity threats through public-private efforts in addition to increasingly tight cybersecurity regulations. These efforts continue to be strong drivers for cybersecurity and data protection in the market.

The General Data Protection Regulation (GDPR) has had global impact. It is enforceable across the European Union and has inspired similar regulation in other parts of the world. The regulation strikes a balance on data collection and processing that puts individual interests first. Strict cybersecurity requirements are also enforced through sector-specific regulations, such as the Network and Internet Security directive. By October 2024, critical infrastructure organizations must have implemented NIS2—the Network and Information Security directive that holds the board liable for the cybersecurity in their organization. The directive also holds organizations accountable for the security of their supply chains.

The Digital Operational Resilience Act (DORA) is coming into force in January 2025 and applies to financial institutions. It requires organizations to demonstrate how quickly they can recover from a cyber attack and to implement employee training.

The EU also regulates the use of AI via a similarly comprehensive approach. A provisional agreement for the EU AI Act was reached in December 2023, but the act won't come into force until 2025. The AI Act describes a risk-based approach to AI with categories for unacceptable risk, high risk, limited risk or minimal risk. Fines can be draconian at 35 million EUR or 3% of gross revenue (whichever is higher).

Organizations may quickly translate new requirements into internal policies, but once these are documented, signed and circulated, they must confront the challenges of cybersecurity governance. It is critical to ensure that organizations and their leaders are unified in their cybersecurity strategies and objectives, with standardized processes, robust enforcement, clear accountability and oversight from senior leaders, along with the necessary resources. To truly strengthen their cybersecurity posture, organizations must implement comprehensive governance. Otherwise, compliance will be nothing more than a checkbox exercise.

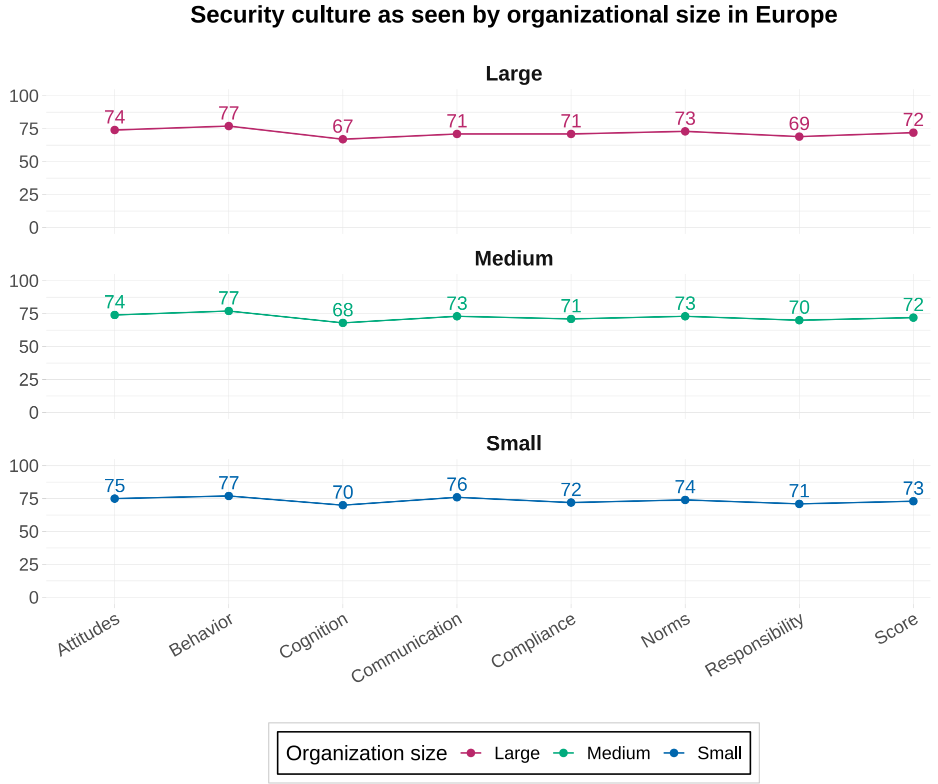
Security Events/ Prevalent Issues

The European Union Agency for Cybersecurity (ENISA) reports an increase in quality and quantity of cyber attacks and their consequences, a surge in ransomware attacks for 2023, and influences from the Russia/Ukraine conflict. The top three threats were ransomware, malware and social engineering. 2023 also saw an increase in professionalization of as-a-service cyber crime offerings, with diversifying tactics and methods fueling alternative ways to infiltrate victims and extort money. Social engineering grew considerably, with phishing remaining the top attack vector while attacks also increased in the physical world.

As highlighted by the Russian war in Ukraine, misinformation and disinformation are on the rise again. Due to upcoming elections in 2024 and the availability of generative AI tools, the quantity and quality of disinformation will continue to pose a threat to society. Generative AI also paves the way for cheap fakes and voice phishing, both of which are increasing threats to private organizations and have been used successfully to extort money.

The MOVEit breach affected insurances, banks and account-switching services across Europe. More than 100 organizations have been affected by the breach that originated from a zero-day vulnerability in the file-sharing service. While the breach has resulted in the SEC tightening reporting guidelines in the U.S., in Europe credit score agencies such as Experian advised customers to freeze credit scores and banks disclosed the leak of customer data including account numbers.

The Clop gang's extortion scheme has also led to further consideration of insurance coverage and payout conditions. Conventionally, ransomware gangs extorted money by encrypting data. The Clop gang demands payment based on the threat of publishing data. However, insurers will not be able to pay out for the purpose of hiding a data breach from authorities. For the actual reporting requirement, this is irrelevant since the breach happened as soon as the gang downloaded the data. Still, reputational damage from a data leak can be significant.



Europe vs. Worldwide

Organizational Size	Attitudes	Behaviors	Cognition	Communication	Compliance	Norms	Responsibilities
Large	75	77	68	72	73	74	69
Europe difference	-1	0	-1	-1	-2	-1	0
Medium	75	75	69	74	73	73	69
Europe difference	-1	2	-1	-1	-2	0	1
Small	75	75	71	77	73	74	71
Europe difference	0	2	-1	-1	-1	0	0

Dimensions

Our 2023 European data set was collected from a total of 673 organizations and 162,688 individuals. The overall security culture score for Europe stands at low-moderate 73, unchanged from prior year.

In Europe, it still holds true that the smaller the organization, the higher the security culture score. Smaller organizations benefit from more personal and efficient communication. Communication channels are perceived as better, and there is a stronger sense of belonging and more support for security issues. Relatedly, Cognition and Compliance are also better.

Among European respondents, there is less understanding of security policies and the extent to which employees are meant to follow them (the Compliance dimension). Similarly, there is less understanding, knowledge and awareness of security issues and activities (the Cognition dimension). It seems possible that the best way to influence these dimensions might be to improve Communication, which is also lacking in Europe. Setting up better communication channels and fostering more open and direct communication can help.

Interestingly, the behavior of people in Europe is reported as more secure in medium and small organizations than the worldwide average. Employees are more likely to act directly or indirectly in ways that improve the security of their organization. Increased legislation and governance, the ensuing threat of the Russia/Ukraine war, and local governments' increased investment in cybersecurity and awareness efforts all contribute to this.

Language Localization

Language localization remains a major factor in Europe, where more than 200 languages are spoken. Moreover, European and national-level legislation posit specific compliance and legal requirements. Localization beyond simple translation and implementation of specific requirements is also necessary. Present cultural differences across the continent do make a difference in human-focused efforts.

AI Influences

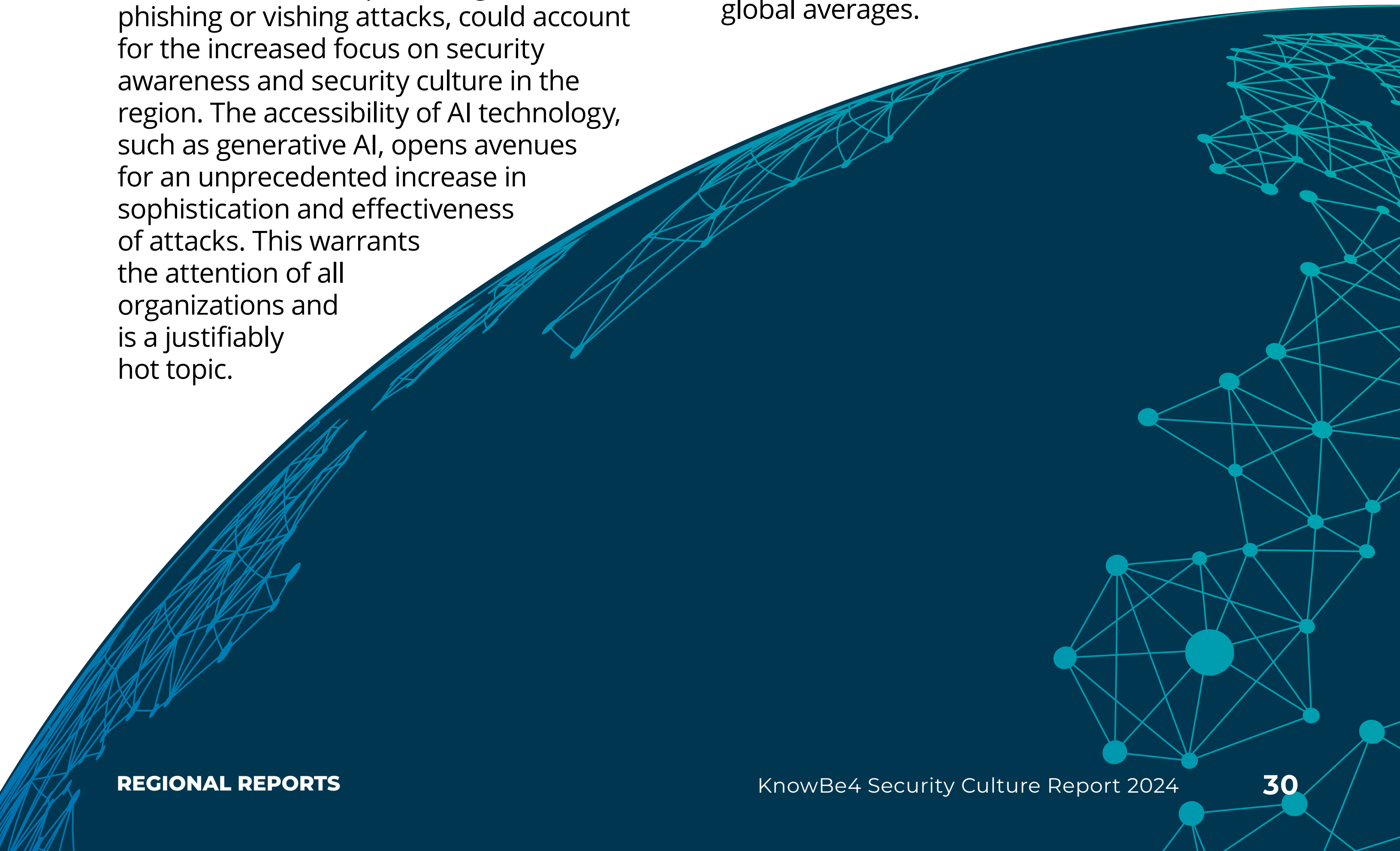
We can report similar influences of AI in Europe as in the rest of the world. The cybersecurity threat landscape evolves with phishing attacks gaining in quantity and quality. Misinformation and disinformation will also be fueled by generative AI, which ENISA already considers a cybersecurity threat. Misinformation campaigns are often used as precursors for other attacks.

And while still relatively uncommon, the possible threat from AI-driven cyber attacks, such as deepfake-augmented phishing or vishing attacks, could account for the increased focus on security awareness and security culture in the region. The accessibility of AI technology, such as generative AI, opens avenues for an unprecedented increase in sophistication and effectiveness of attacks. This warrants the attention of all organizations and is a justifiably hot topic.

AI also continues to affect businesses. In a traditionally compliance-driven region, the uncertainties of AI's impact on the workforce and the nature of work as well as far-reaching ethical considerations are likely to slow adoption. While the EU AI Act is supposed to provide a framework and legal surety, it is controversial even before coming into effect. Legal and regulatory guardrails normally result in a slower, more purposeful adoption of new technologies. That said, very few businesses will continue to resist the promises of increases in productivity long term.

Key Takeaways

Smaller European organizations score higher in security culture due to more effective personal communication, stronger community bonds and better support for security issues. This leads to enhanced Cognition and Compliance, with improvements in communication channels posited as a key driver for better security policy understanding and proactive security behaviors that outperform global averages.



Security culture in Europe exhibits significant variation in understanding and adoption across industries, with a general trend toward increased awareness in highly digitized sectors. However, many organizations have yet to make substantial strides in developing a proactive security culture. European organizations are recognizing the strategic importance of integrating security awareness into their corporate culture to enhance resilience. However, challenges persist where cybersecurity is not yet viewed as a cross-departmental responsibility.

The EU is at the forefront of shaping global cybersecurity standards through robust legislation and regulations like the GDPR, sector-specific directives such as NIS2, and upcoming comprehensive policies including DORA and the EU AI Act. ENISA identifies a notable escalation in cyber attacks during 2023, with ransomware, malware and social engineering as top threats. These are exacerbated by professional as-a-service cyber crime offerings and physical attacks.

Generative AI-driven misinformation is becoming a growing concern, while significant breaches like MOVEit and Clop gang's extortion tactics are influencing cybersecurity reporting regulations, credit security measures and insurance industry responses to ransomware and data leaks.

In Europe, the diversity of 24 official languages and distinct legislative frameworks necessitate meticulous language localization and culturally nuanced compliance strategies to effectively address the varied human-centric aspects of cybersecurity efforts across the continent.

AI's influence on Europe echoes global trends with a rise in sophisticated phishing and use of generative AI for misinformation now recognized as a cybersecurity threat by ENISA. This compliance-centric market and its caution around AI's ethical implications and workforce impact could slow adoption even as businesses ultimately seek the productivity gains AI promises.

Asia

By Martin J. Kraemer, Security Awareness Advocate

Cultural Adoption

The Security Culture Report encompasses data from 27 diverse nations across five distinct areas and reveals significant disparities in security culture scores. Notably, the Middle East and East Asia exhibit a higher degree of maturity in their security cultures compared to their counterparts in Central, South and Southeast Asia.

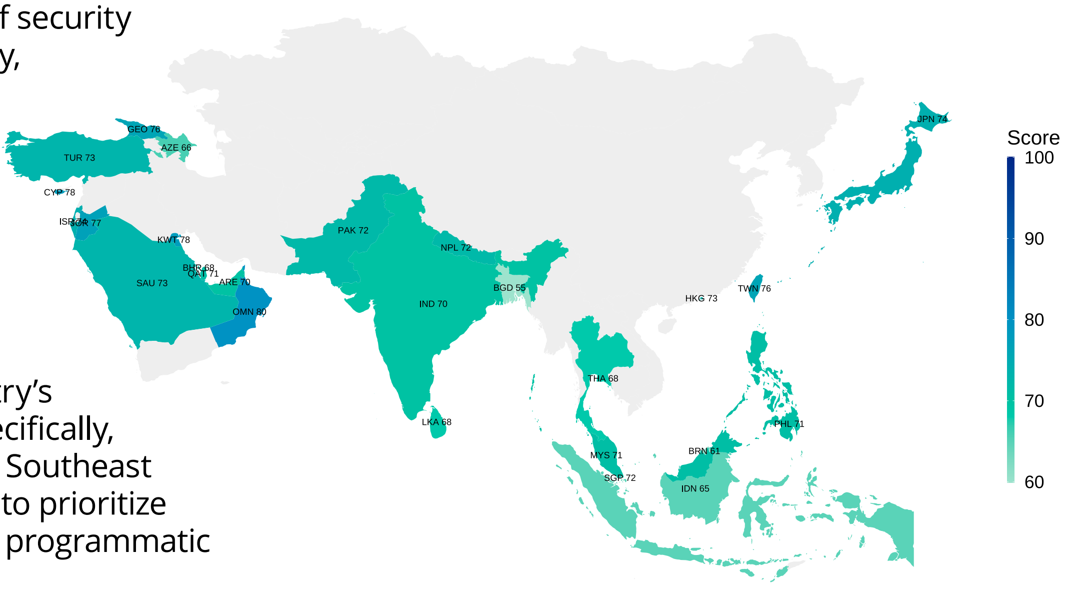
This variance highlights the presence of countries within the region whose security practices are comparable to those of European nations. However, there exists a notable gap in legislation, technical and organizational maturity when compared to European and North American standards. The cybersecurity infrastructure in several of these nations is underdeveloped. Socioeconomic disparities among these countries likely influence their security culture scores. Investments in the social and cultural dimensions of security could enhance their overall security stance, as indicated by research findings.

The analysis reveals that only a few countries and industries within this region meet the global average, pointing to a widespread lack of awareness and appreciation for the importance of security culture. Consequently, organizations within these nations may find it necessary to significantly invest in enhancing internal awareness and advocating for collaborative efforts to improve the country's security posture. Specifically, nations in South and Southeast Asia are encouraged to prioritize the establishment of programmatic awareness initiatives as a precursor to fostering security-conscious behaviors.

With 48 sovereign countries, Asia is home to 4.6 billion individuals who speak over 2,300 distinct languages. Mandarin, Hindi, Indonesian, Bengali and Japanese are among the most prevalent. This linguistic and cultural diversity further complicates the challenge of establishing a unified security culture across the continent, underscoring the importance of tailored and inclusive approaches to cybersecurity education and awareness.

Region	Avg. Security Culture Score	Number of Organizations
Central Asia	66	1
East Asia	74	22
Middle East	74	51
South Asia	68	19
Southeast Asia	68	64
Grand Total	**71**	**157**

Security culture in Asia



General Attitudes

Attitudes toward cultural adoption and cybersecurity differ from one country to another, influenced by each country's laws and regulations. All countries, without exception, are impacted by cyber crime. This impact correlates to the number and size of organizations that exist within each country.

In Asia, high-context communication styles prevail. Direct messages often fail to resonate because they do not align with local cultural expectations. Those specializing in raising cybersecurity awareness need to tailor their strategies: effective communication must be not only clear and direct but also convey the right tone, style and context.

Asian cultures tend to have a more pronounced sense of social norms and hierarchies than European or North American cultures. Leveraging these norms and structures could help alter the prevalent organizational mindset regarding cybersecurity. Currently, cybersecurity is often viewed as solely a concern for IT departments. It's essential for professionals in the field to help shift this perception toward cybersecurity as everyone's responsibility.

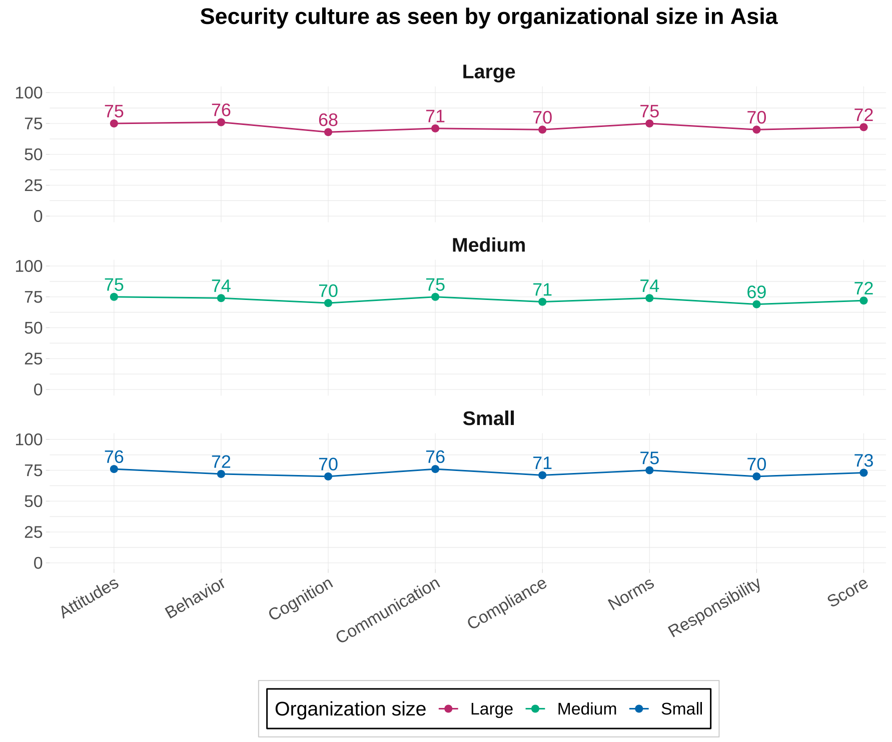
Key Regulatory Requirements (i.e., Legislative)

Regulatory requirements are usually driven by cohesive cybersecurity strategies. However, many countries in the region are yet to develop their own vision for cybersecurity. As such, the regulatory landscape is fragmented, and there is no effort to create unified cybersecurity standards across the area.

The Association of Southeast Asian Nations (ASEAN) released their 2021-2025 ASEAN Cybersecurity Cooperation Strategy, which provides a "roadmap for regional cooperation to achieve the objective of a safe and security ASEAN cyberspace." ASEAN includes the member states of Brunei Darussalam, Cambodia, Indonesia, Myanmar, Lao PDR, Malaysia, Philippines, Singapore, Thailand and Vietnam.

Singapore's Cybersecurity Act has been in force since 2018, and on December 15, 2023, the Cyber Security Agency of Singapore (CSA) published a consultation paper on a draft Cybersecurity (Amendment) Bill 2023 (Bill).

Regulatory requirements in the regions are challenging. India forces organizations to report data breaches within six hours from the moment of discovery. Naturally, this requirement is criticized as impractical by experts. Criminal charges and hefty fines are waiting should this requirement not be met. Other countries in the region have introduced legislation to enforce local data storage.



The regulatory landscape in the region will stay very fragmented for the foreseeable future. Organizations doing business in the region must therefore be prepared to adhere to ever-evolving country-specific legislation. Staying up to date with that legislation becomes a major task for professionals.

Security Events/ Prevalent Issues

Cybersecurity challenges such as ransomware, data breaches, and AI-enhanced threats are common globally, including in Asia. These problems have led to calls for updated reporting laws and new regulations throughout the region. Notably, Singapore saw a sharp increase in QR code phishing scams in 2023, and this trend is expected to persist into 2024.

The Allianz Commercial Risk Barometer for 2024 identifies cyber risk as the primary concern for businesses in the Asia Pacific region, with malware, ransomware, and social engineering attacks being the most common attack strategies. Criminals often use emails, websites and social media for these deceptive attacks.

Reports highlight that Asia is facing a particularly high surge in cyber attacks compared to other regions, making it a prime target for cybercriminals. This surge is attributed to the region's rapid digital growth, strong manufacturing sector, and burgeoning population of new tech users. To combat this, there is a dire need for more investment in national cybersecurity policies and the formation of dedicated cyber task forces. In addition, enhancing education and training on this front is becoming increasingly urgent.

Dimensions

Organizations in Asia generally exhibit lower cybersecurity behavior scores regardless of size, and they also tend to score lower on Compliance measures. This trend may translate into a weaker overall cybersecurity stance, with employees being less inclined to follow security guidelines or to act in a secure manner. However, Asia is known for its strong social traditions, which is likely why the region performs better when it comes to social norm-related aspects of security. Security professionals should prioritize establishing robust security policies and collaborate with different departments to foster positive norms that encourage secure behavior.

Organizational size (Global overview)	Attitudes	Behaviors	Cognition	Communication	Compliance	Norms	Responsibilities
Large	75	77	68	72	73	74	69
Asia difference	0	-1	0	-1	-3	1	1
Medium	75	75	69	74	73	73	69
Asia difference	0	-1	1	1	-2	1	0
Small	75	75	71	77	73	74	71
Asia difference	1	-3	-1	-1	-2	1	-1

We can also see that the leading industries with security culture scores over 73 are highly regulated. They are Government (74), Energy and Utilities (74), Banking (74), Manufacturing (73) and Financial Services (73). At the other end of the spectrum, industries with low security culture scores include Construction and Legal (68 for both) and Education (69). These industries would be advised to focus on areas of improvement within the security culture dimensions if they are to make a positive impact moving forward.

Language Localization

With around 2,300 languages spoken by 4.46 billion people across Asia, language localization is critically important to uptake and engagement of both organizations and employees. This brings challenges in ensuring not only the availability of local languages, but also in addressing nuances and cultural differences within security awareness programs.

In Asia's high-context cultures, effective communication goes beyond words. To convey messages about cybersecurity successfully, one must consider communication style, tone and language nuances. Messages should be rich in context and not purely straightforward or blunt, as this approach resonates better within the region. Moreover, since Asian cultures often value hierarchy, a top-down communication approach may be appropriate and effective. It's vital to be mindful of cultural nuances when trying to influence security practices and attitudes.

AI Influences

Like all technologies, AI presents both great opportunities and threats regarding cybersecurity. AI isn't new. What is new is the advancement of deepfake technologies and large language learning models, such as ChatGPT, with the addition of voice, image and video generation. These new advancements introduce additional potential red flags. Cybercriminals are still focusing on attaining the human emotional response with social engineering.

Organizations and individuals are concerned with AI and how it has added a new strain of cyber crime, which has devastating effects. Calls continue for more regulation and legislation in this space to protect the region from AI. Released in January 2024, The Engaging with Artificial Intelligence (AI) report is a collaboration among 13 international organizations, including the Cyber Security Agency of Singapore (CSA) and other Asia-based organizations.

Key Takeaways

The many countries across Asia require a collaborative approach to cybersecurity. There is a large disparity between the Middle East and East Asia and other parts of the region. This is largely due to socioeconomic differences in the countries. While some countries are already working together, there is an opportunity for greater success with additional collaboration and resource sharing if the region is to increase its cybersecurity awareness and strengthen its overall security culture.

Oceania (Australia, New Zealand and Papua New Guinea)

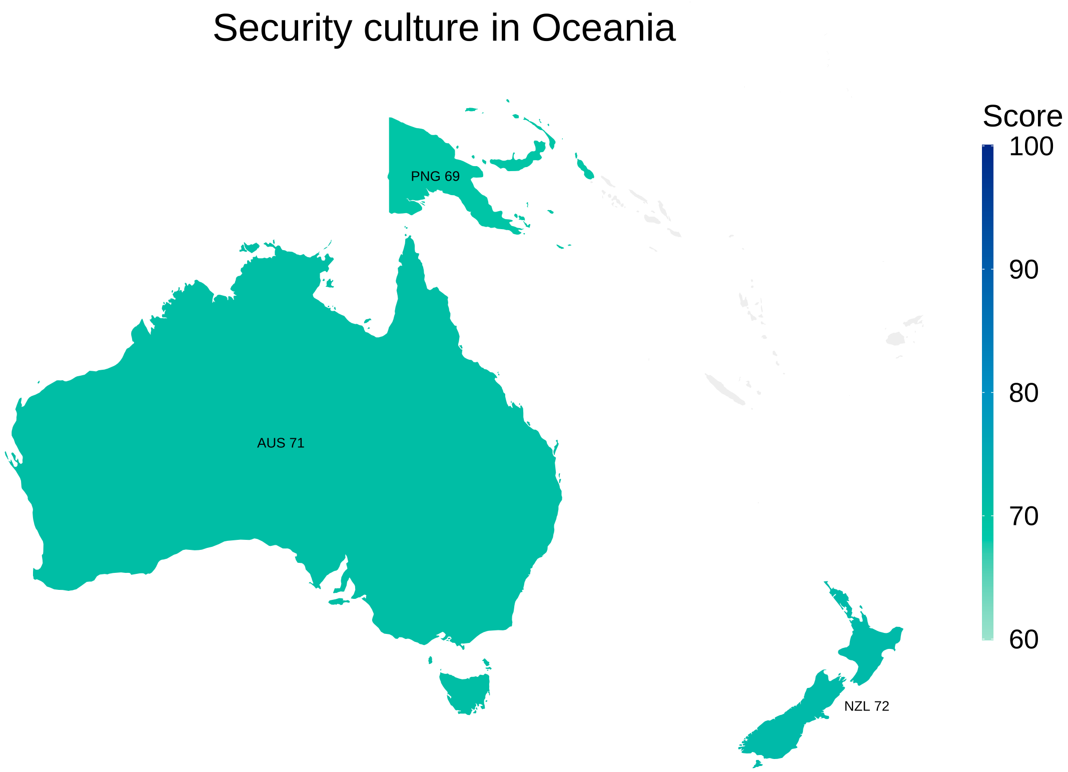
By Martin J. Kraemer, Security Awareness Advocate

Cultural Adoption

Security culture has increased year over year as a topic of interest in the region with a welcome addition of business units outside of IT, such as HR, at the table. IT acknowledges the requirement for change management principles aligned with cybersecurity strategy to engage employees' hearts and minds. Over the past 12 months, we have also seen an increased demand and understanding of cybersecurity at the board level, with cybersecurity now accepted as a business risk rather than an IT risk.

Developments like these illustrate that Australia and New Zealand are making important strides toward maturing cybersecurity culture overall. The Oceania Cyber Security Center has determined that the technological abilities of the region far exceed the human capabilities in 2021. Subsequent initiatives have improved the situation, but as the security culture score shows, the region still has catching up to do.

Australia and New Zealand are the most developed economies in the region, and they show the best security scores. For reference, the ITU Global Cybersecurity Index ranking from 2020 places Australia 15th, New Zealand 32nd and Papua New Guinea 149th. The region includes 14 independent countries and several overseas territories. It is estimated that people in the region speak more than 1,200 languages. Our dataset includes organizations in Australia (133), New Zealand (29) and Papua New Guinea (3).



General Attitudes

As a result of significant data breaches in the region, the line between work and personal cybersecurity has blurred. Most citizens have experienced a breach of their Personally Identifiable Information. Scams, breaches, and ransomware have become daily occurrences across all media platforms, normalizing the topic. The Australian government continues to raise awareness through campaigns, such as “Stay Smart Online” or “Get Cyber Smart.”

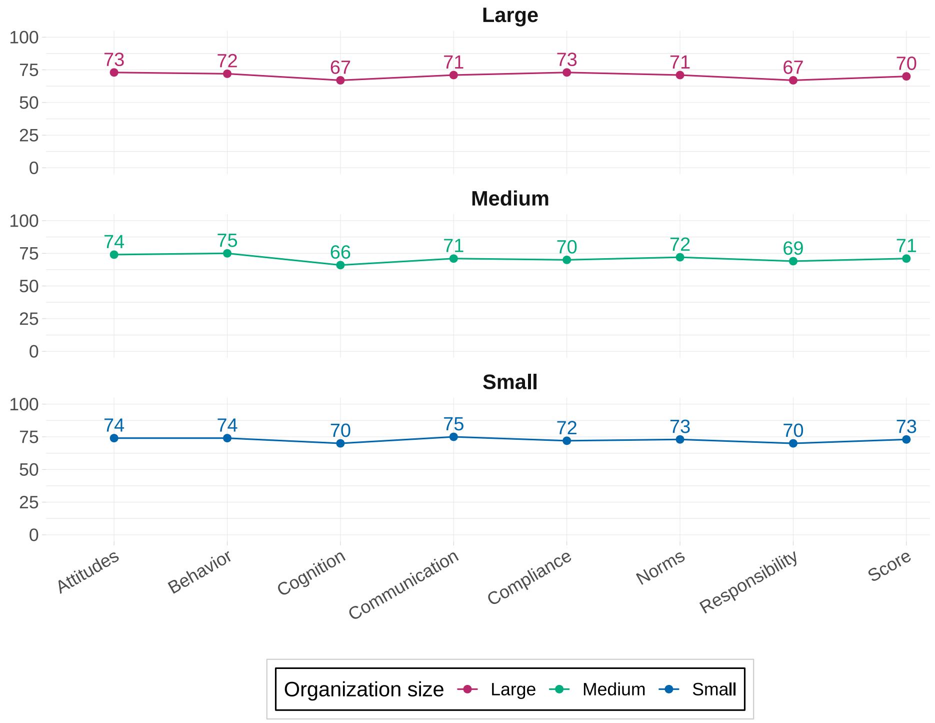
Social engineering and phishing attacks are the most common threats, highlighting the need for continued training and increased awareness. Calls for stronger defense mechanisms are also fueled by the continued threat of ransomware attacks on businesses and critical infrastructure. There are efforts to combat that threat through public-private collaboration between businesses and government bodies.

Key Regulatory Requirements (i.e., Legislative)

Australia and New Zealand have updated and implemented new regulatory requirements in 2023. The 2023-2030 Australian Cyber Security Strategy was released in late 2023. The strategy is intended as a roadmap to help realize the Australian government’s vision of becoming a world leader in cybersecurity by 2030. In addition, a mandatory data breach notification scheme is a hot topic across Australia. In August, New Zealand released its National Security Strategy 2023-2028, which is an extension of its 2019 Cyber Security Strategy.

Both strategies are set to transform the cybersecurity landscape significantly by motivating organizations to boost their efforts in becoming more cyber resilient. These strategies draw parallels with the U.S. approach by promoting collaboration between the public and private sectors for enhanced defense and positioning major businesses at the forefront of Australia’s cyber defense initiatives. Additionally, organizations are now subject to mandatory reporting obligations and should anticipate further regulatory updates shortly. The goal is to elevate Australia’s cybersecurity readiness to meet robust international standards.

Security culture as seen by organizational size in Oceania



Security Events/ Prevalent Issues

In 2023, the Oceania region witnessed several high-profile data breaches, significantly impacting its citizens, sometimes repeatedly, and leading to class-action lawsuits. For instance, in March 2023, Latitude Financial reported a massive data breach involving 12 million customer records in Australia and New Zealand, exposing sensitive details like driver's license and passport numbers. This incident was one of the largest in recent times. Following closely, the telecommunications giant Optus experienced a breach affecting 9.8 million customers, and Medibank's breach compromised 9.7 million health records and personal information.

These incidents, alongside the growing use of ransomware, data breaches and the advanced capabilities of generative AI, are major concerns for IT professionals in the region. These challenges underscore the urgent need to reassess and update current data breach reporting laws and the Privacy Act. Moreover, the emergence of generative AI has sparked a call for new rules and laws to protect organizations and individuals alike.

Dimensions

The KnowBe4 security culture average score of 71 for the assessed organizations from three countries across Oceania shows a moderate level of security culture aligned with the rest of the global regions.

As we focus on the specific sectors across Oceania, not surprisingly, Technology is leading the way with a security score of 77, above the regional average. Alarmingly, there are six sectors scoring 70 or under: Government (70), Construction (70), Banking (70), Energy and Utilities (69), Education (69), and Healthcare and Pharmaceuticals (67).

The dimension of Cognition is low in both Australia (69) and New Zealand (67), which may indicate a lack of ongoing training that would otherwise increase understanding, knowledge and awareness. Overall, the region falls behind the global average, indicating a potential to mature security culture across organizations. Our insights are in line with the ITU's Global Cybersecurity Index and similar reports that highlight needs for development of cybersecurity capabilities in Australia and New Zealand as the most developed countries.

Organizational size (Global overview)	Attitudes	Behaviors	Cognition	Communication	Compliance	Norms	Responsibilities
Large	75	75	68	72	73	74	69
Oceania difference	-2	-2	-1	-1	0	-3	-2
Medium	75	75	69	74	73	73	69
Oceania difference	-1	-1	-3	-3	-3	-1	0
Small	75	75	71	77	73	74	71
Oceania difference	-1	-1	-1	-2	-1	-1	-1

Language Localization

Adapting content to local language and culture is crucial in Australia and New Zealand, especially in Communication-related areas such as cybersecurity training. For instance, even the spelling differences between "localization" and "localisation" highlight the importance of using a genuine Australian or New Zealand voice in training materials. Recognizing such regional nuances can significantly enhance acceptance and appreciation. Tailoring the cybersecurity message with local language adaptations leads to better employee engagement and commitment, key factors in developing a strong security culture.

Moreover, the Oceania region is incredibly diverse in terms of language and culture. Australia, while primarily English-speaking, is home to numerous indigenous languages and languages brought by immigrants. New Zealand recognizes five official languages, along with several indigenous languages. Papua New Guinea stands out with a staggering 800 indigenous languages alongside English and Tok Pisin as official languages. This rich cultural tapestry underscores the need for inclusivity and sensitivity in training materials to ensure they resonate across this varied linguistic landscape.

AI Influences

Organizations and individuals across the region are concerned with AI and how it has added a new avenue for cyber crime with potentially devastating effects. While there is no argument that AI can also have positive effects on all areas of life, it comes with a quick introduction of deepfakes in images, voice and video adding complexity to existing social engineering red flags. With these advancements, the increase of the emotional human response needs to be addressed.

There is a call for more regulation and legislation in this space to protect the region from AI-related threats and misuse. The Australian Government published its interim response to supporting responsible AI on January 17, 2024.

The Engaging with Artificial Intelligence (AI) report was released in January 2024 and is a collaboration between 13 international organizations, including New Zealand's CERT NZ, the National Cyber Security Centre, the Australian Signals Directorate and the Australian Cyber Security Centre.

Key Takeaways

Conversations about security culture are attracting the attention the topic deserves across organizations, and we have seen a resulting increase in best-practice security awareness training programs. These programs are influencing other organizations to reexamine their programs and make appropriate adjustments.

As more citizens in the region fall victim to cyber incidents, demand for legislation, regulations, data protection, privacy and knowledge increases.

AI has certainly added complexity to cyber crime. Individuals need additional understanding to keep it in perspective while adding relevant red flags to their awareness bank.

Industry Benchmark

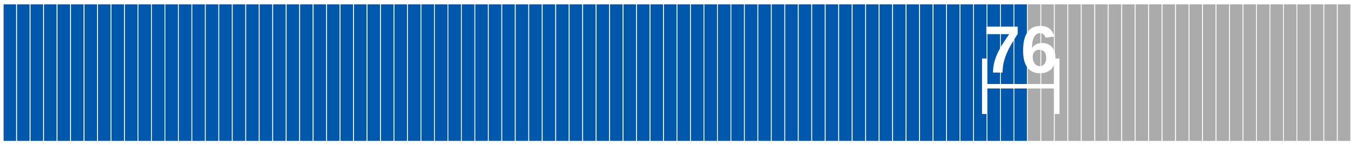
In this portion of the report, we present an in-depth examination of security culture ratings spanning multiple industry sectors. Use this thorough analysis to deepen your understanding of specific industries and employ it as a benchmarking tool to assess your organization's security culture against industry-wide standards. This segment also enables a side-by-side comparison of your sector's security standing with that of others, providing a robust framework for a benchmarking evaluation.

Security culture exhibits significant variation across different sectors. Within the industry comparison section of the report, we conduct an evaluative analysis of each based on their respective security culture scores, as well as a cross-sectional analysis against seven dimensions that constitute security culture.

Industry Benchmark Guide

Industry Benchmark Score

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



43,586

Number of Employees

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

212

Number of Organizations

This is the number of organizations in this industry.

75 76

Year-Over-Year Trend

This shows this year's score (on the right) compared to the previous year's score (on the left).

Banking

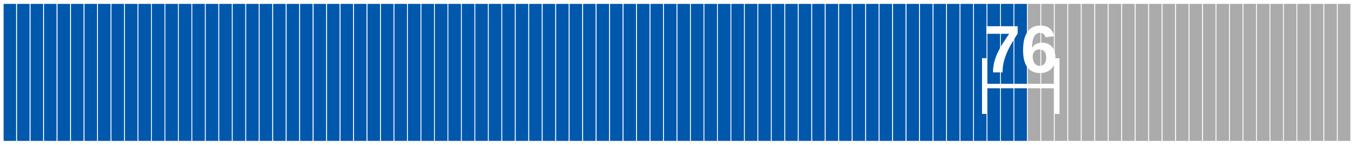
The Banking sector recognizes risk management principles due to the high stakes involved with financial data. Mandated cybersecurity standards and employee training protocols contribute significantly to this sector's comprehensive risk management strategy. It has achieved an improved security culture score of mid moderate 76 compared to the previous year, a testimony to consistent effort over time.

Benchmarked with the previous year's employee survey results, minor shifts have been observed in some dimensions. The Norms dimension, with a two-point rise to 76 from the last measurement period, indicates a subtle shift in overall security culture considerations.

The financial sector, unfortunately, bears the brunt of any successful breach, not only financially but also in terms of trust, with an institution's reputation often tainted among its customers and the broader public. Ransomware, a threatening type of malware, is the primary driver of these high-impact digital incidents.

In January 2023, an industry consortium warned about the rising prevalence of distributed denial-of-service (DDoS) attacks. The consortium called for increased vigilance among banks and credit unions to prevent these already disruptive attacks from becoming a regular occurrence.

A researcher observed that the landscape of cyber threats evolved in 2023. Banking trojans, ransomware and deceptive finance apps designed for data theft have been the tools of choice for cybercriminals. According to a survey carried out by the researcher, 60% of institutions confirmed falling victim to destructive attacks within the year, while 64% experienced a surge in application attacks. Software development, integration and delivery infrastructures are facing an increasing threat from adversaries targeting supply chains.

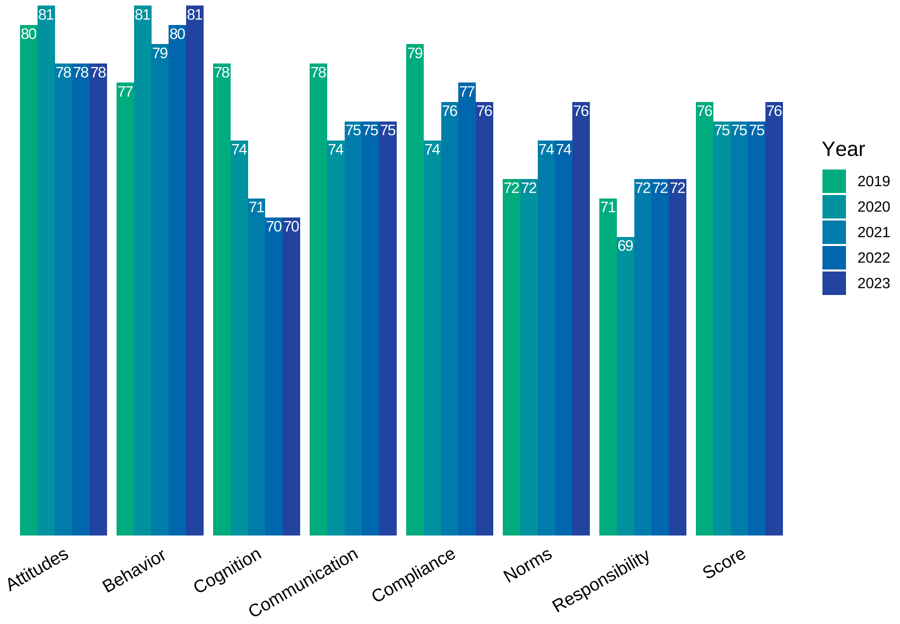


212

43,586

75 76

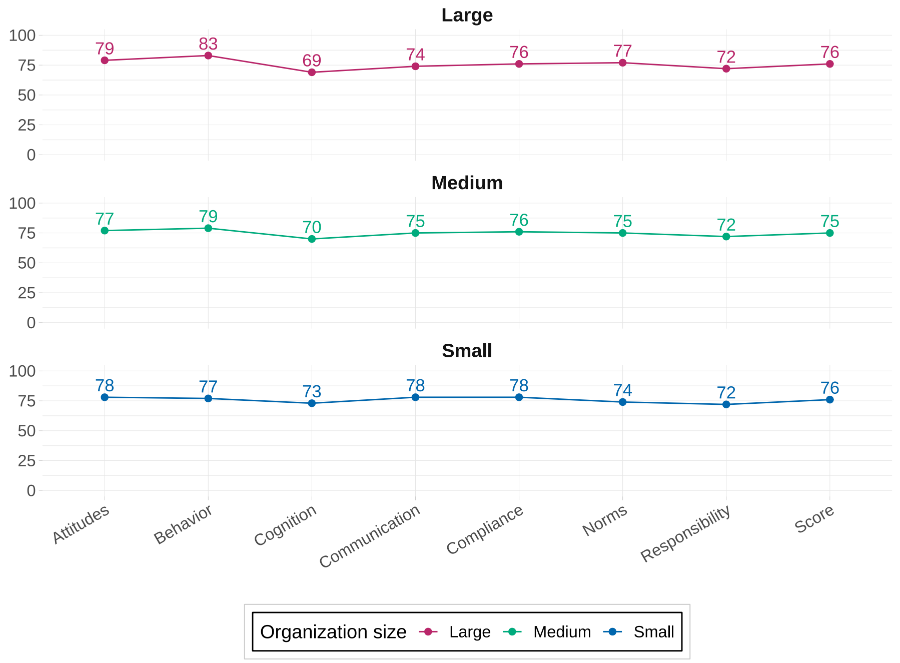
Security culture trends across all dimensions in Banking



Areas for Improvement

Despite steady ratings on Attitudes, Communication and Responsibilities (78, 75, and 72, respectively), Cognition continues to be the lowest-scoring dimension at low moderate 70. A particular focus on enhancing Cognition and Responsibilities within the Banking sector's security culture could be beneficial, especially with the ever-looming threat of ransomware.

Banking

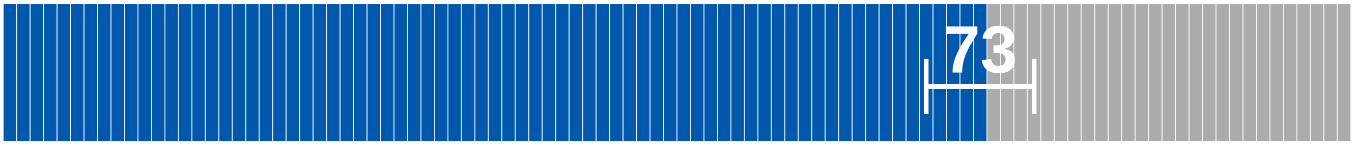


Business Services

The Business Services sector, encompassing a diverse array of professions from recruitment and physical security to office management and sanitation, underscores the universal risk of cyber attacks no industry can ignore.

Despite a slight dip in the security culture score to a mid moderate 73, the sector's risk level has held steady over the past half-decade at a low moderate range. Vulnerabilities arise from minimal security protocols, outdated IT systems, and a tendency to acquiesce to ransom demands for customer data recovery. Cybercriminals capitalize on these weaknesses, aware of the sector's often insufficient understanding of their vendors' security measures. Additionally, the sector's reliance on a remote workforce, relationship-driven operations, and challenges in establishing continuous training and awareness heightens its appeal as a target for cyber threats.

In this year's Security Culture Index, the dimensions of Behaviors (76) and Attitudes (75) maintain a mid-moderate standing, indicating that employees generally make secure choices and demonstrate a readiness to adopt behaviors that positively influence organizational security. However, the areas of Cognition (70) and Responsibilities (70) reveal a gap: while there's a willingness to enhance security, there's an apparent shortfall in understanding effective implementation. This disconnect has significant implications, as highlighted by alarming developments in data security. Security Discovery and CyberNews researchers have uncovered a staggering database breach, involving over 26 billion compromised records, including information from LinkedIn, a key platform for professional recruitment.

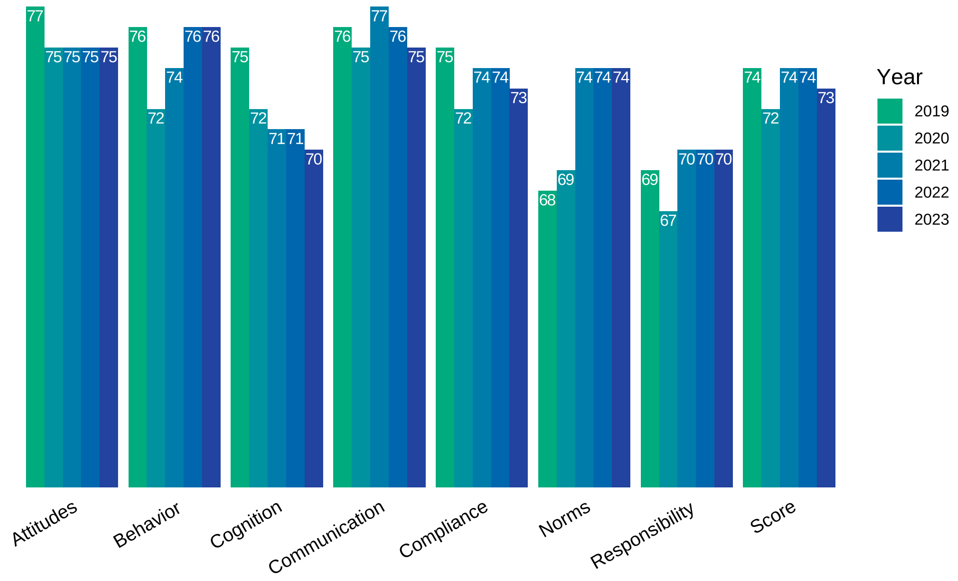


359

49,003

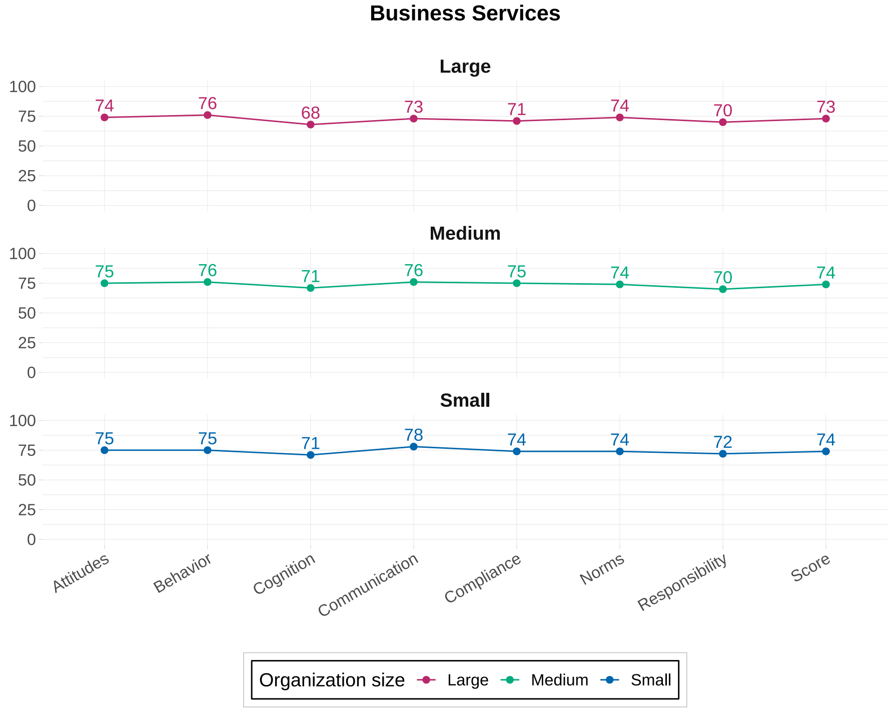
74 73

Security culture trends across all dimensions in Business Services



Areas for Improvement

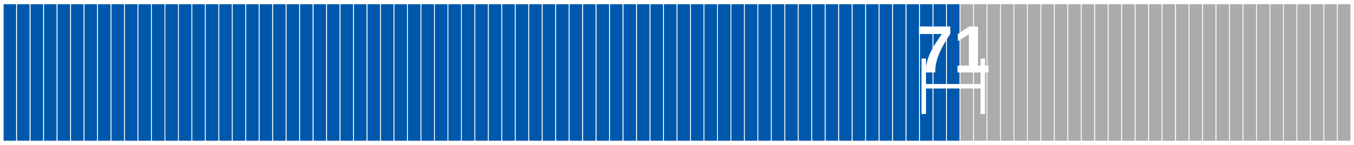
The Business Services sector stands to gain significantly by bolstering its dedication to ongoing, holistic training and education programs. Enhancing employees' understanding of security will not only improve Cognition scores but also positively affect their perception of personal responsibility in safeguarding the organization.



Construction

In the Construction industry, there has been a significant shift away from conventional business methods toward adopting advanced technologies for collaboration, supply chain management and assessment of on-site work and progress. However, this accelerated integration of technology brings with it the need for greater comprehension of associated risk factors, particularly exposure to cybersecurity threats. Alongside these advancements, the industry faces a persistent labor shortage and high employee turnover that hinders the development of strong personal cybersecurity practices. That leaves the door open for potential cyber incidents. Despite a marginal improvement in the security culture score this year to a barely sufficient low moderate 71, the sector is close to descending into a range indicative of lackluster performance, a trend observed over multiple years.

Intriguingly, in the realm of security culture dimensions, Behaviors and Communication have obtained a score of 73, which is somewhat satisfactory. However, the dimensions of Cognition and Responsibilities, scoring 66 and 67 respectively, are considered mediocre. This disparity highlights a gap where employees receive adequate information but fail to interpret and apply it, leading to a lapse in recognizing their individual roles in maintaining cybersecurity in both their professional and private spheres. As the pace of business quickens and AI becomes more sophisticated, the risk of cyber attacks intensifies. For the construction industry, with its stringent deadlines, high transaction volumes and thin profit margins, any disruption due to a cyber attack can be immensely detrimental, as evidenced by the cyber attack on Simpson Manufacturing in Q4 of 2023. The attack forced a system shutdown and indicates the possibility of a ransomware attack, though specific details were not disclosed.

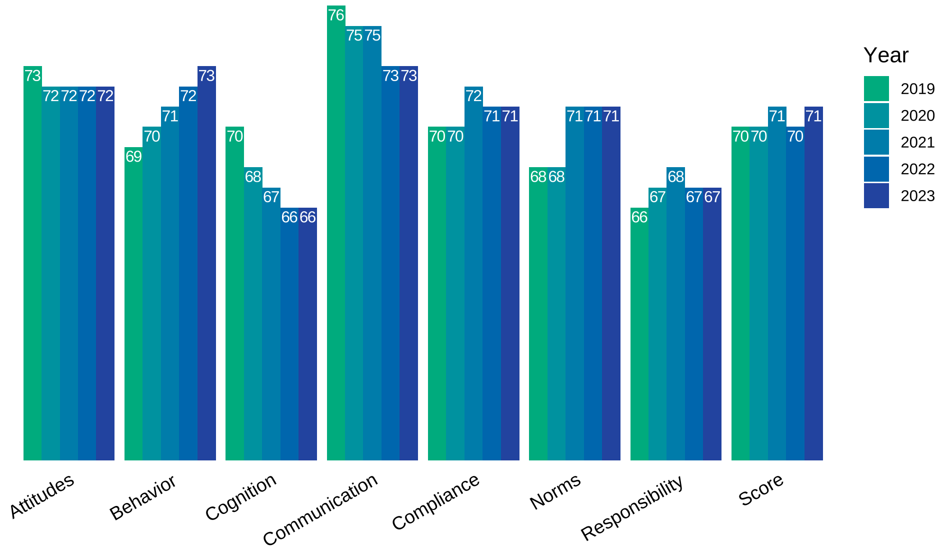


70 71

126

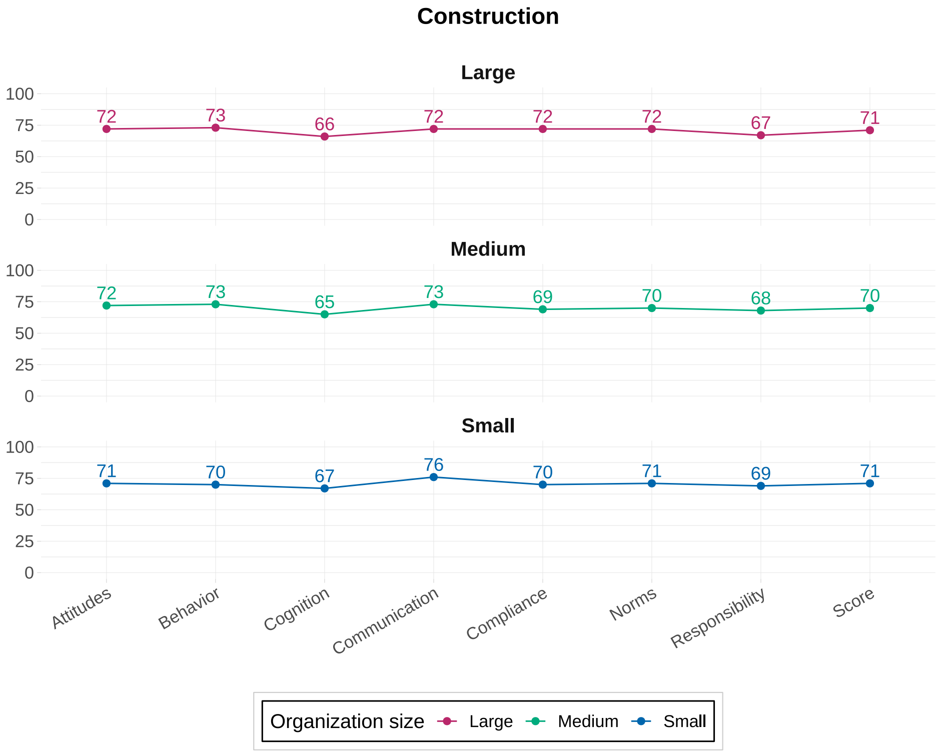
31,238

Security culture trends across all dimensions in Construction



Areas for Improvement

To address these emerging technological realities, construction businesses must prioritize compliance with data regulations and privacy laws to safeguard their intellectual property and client data. They must establish a stronger link between personnel training, cybersecurity awareness and the cultivation of a security-conscious culture.

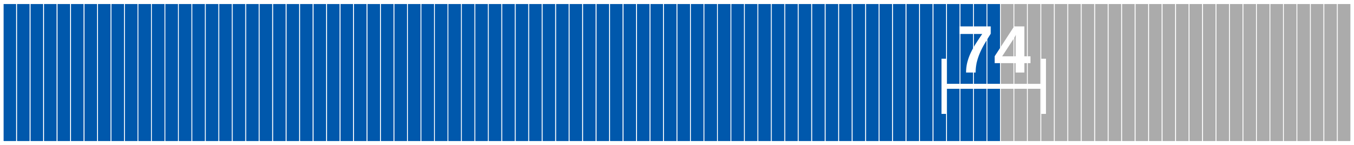


Consulting

The Consulting industry has seen security culture scores remain constant at a mid moderate 75 over the past two years, which signals a period of stagnation. The foundation of a consulting firm's success is the trust placed in it by clients; any breach in that trust can result in severe harm to the firm's reputation and lead to a tangible loss in both existing and potential clientele. By their very nature, consulting entities handle copious amounts of sensitive data, balancing high expectations for confidentiality against the demands of a fast-paced and often stressful work setting. Since they possess valuable client intellectual property as well as vast amounts of sensitive personal and financial information, they present an attractive target for cybercriminals.

On the Security Culture Index, the Consulting sector demonstrates fairly acceptable scores of 76 in Attitudes, Behaviors and Communication, yet it underperforms with a score of 70 in Responsibilities and a somewhat better 72 in Cognition. This suggests that while conversions with security policies and the perception of individual impact on organizational security are present, there is a struggle to engage with wider industry-specific security challenges and to put into practice effective protection and defensive measures. Put simply, while these employees grasp the concept of security, translating that understanding into concrete actions remains an issue. The pressure from cyber threats is anticipated to mount for consulting firms, as exemplified by a reported global ransomware attack that impacted leading firms like PwC and EY, as covered by the Financial Review. Such incidents confirm the growing cyber risks in the sector.

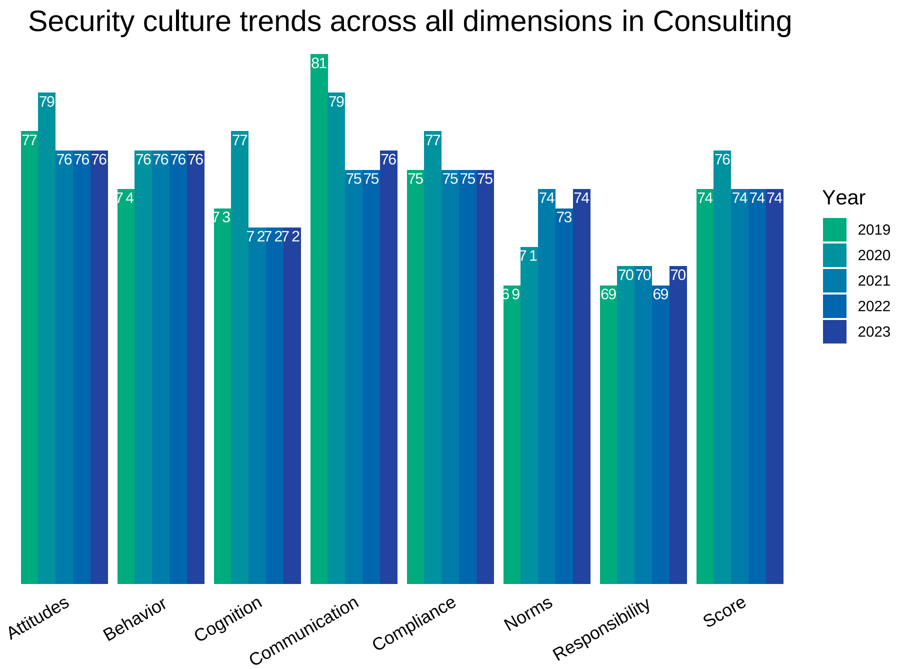
Amid progress in AI technology, which is not expected to replace consultants but to augment their capacity to handle increased workloads, the industry must grapple with the pressures of intensified demand alongside diminished resources. These dynamics could exacerbate employee burnout.



74 → 74

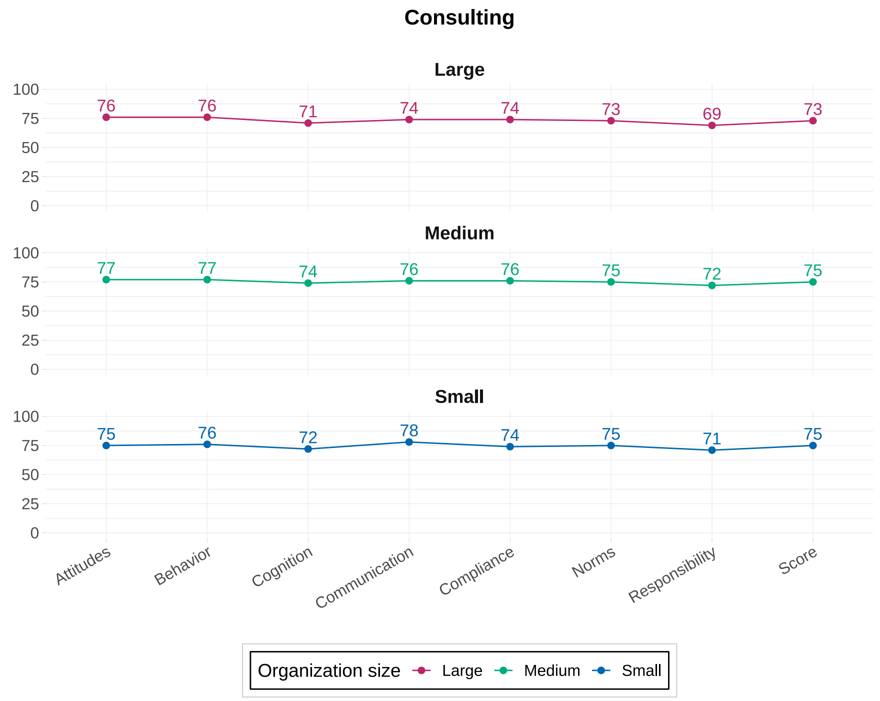
144

16,795



Areas for Improvement

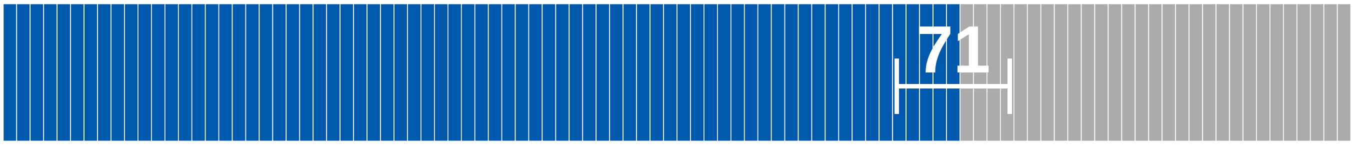
For improvement, consulting firms—particularly large ones offering cybersecurity services—must embody the very security practices they advocate to clients. Leadership should exemplify the desired security behaviors, and by leveraging security champion programs, firms can foster better alignment of security messaging with staff needs to ensure local support and relevance. Mere directives from the top are insufficient in such an environment; instead, leadership should actively demonstrate the significance of nurturing a security-minded culture through actions, not just words.



Consumer Services

The Consumer Services sector's approach to cybersecurity remains modest, with its security culture score dipping slightly to 71 from the previous year, reflecting a low moderate standing. This sector, which spans a broad range of industries such as travel, food and beverage, media and leisure, directly services consumers and encompasses a variety of occupations, including customer service representatives, cleaners, delivery drivers and facilities managers. When assessing the risk landscape, one could compare the challenges of executing a bank heist against exploiting individual consumer accounts; while a bank may offer a larger bounty, it is heavily fortified, whereas individual accounts, though yielding smaller gains, are typically less secure and, therefore, more susceptible to cyber attacks. This inherent vulnerability in consumer-facing systems makes organizations within this sector particularly enticing to cybercriminals.

On the Security Culture Index, the areas of Attitudes, Behaviors and Communication score reasonably yet on the lower moderate side for the Consumer Services sector. However, Cognition and Responsibilities are notably deficient and rated as mediocre, corresponding to the Consulting sector's shortcomings. Despite frequent communication on security from their organizations and a belief among employees that they play a role in safeguarding company security, there is a discernible gap in comprehending the wider security issues relevant to their roles and industry, as well as devising effective protective strategies. Employees know the importance of security, but they often lack clarity on their precise role and the actions they can take. They may unintentionally become the weak link that initiates a cyber threat, as illustrated by the September 2023 cyber attack on the travel booking company Sabre, where hackers claimed to have pilfered extensive amounts of sensitive data.

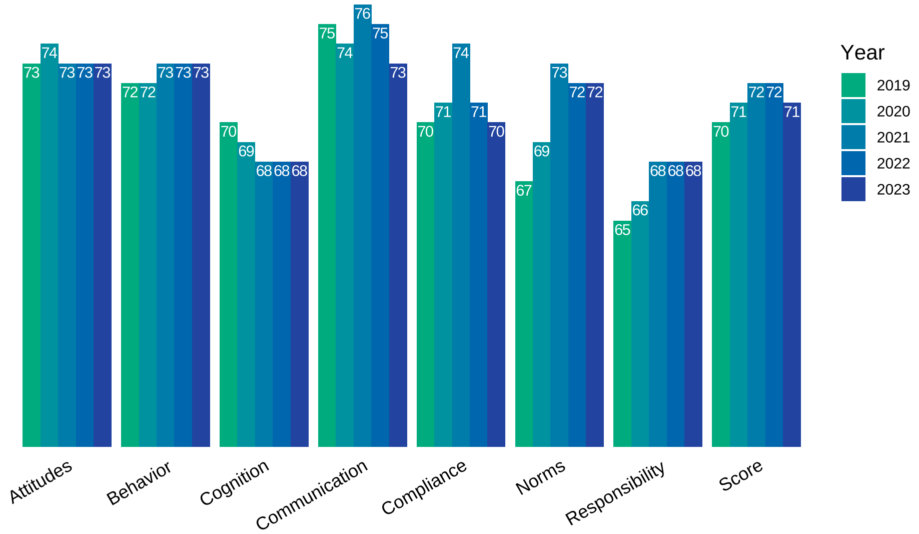


125

15,680

72 71

Security culture trends across all dimensions in Consumer Services



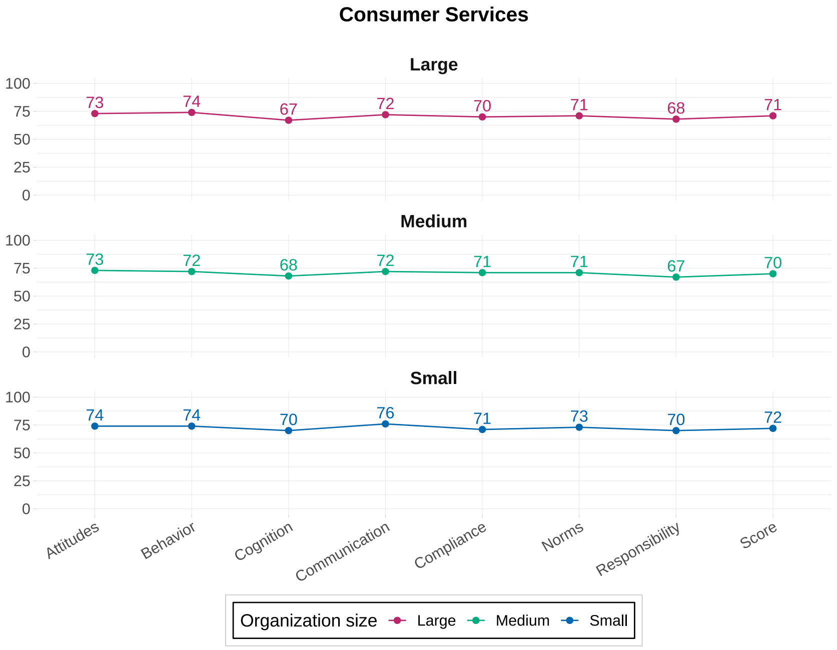
Areas for Improvement

For the Consumer Services sector to fortify its defenses in an era increasingly defined by AI's influence on consumer behavior, priority should be given to:

1. Elevating the security awareness of employees through comprehensive training programs that blend educational content, simulations and consistent communication, empowering them to identify and report suspicious activities.

2. Strengthening internal protective measures by investing in advanced technological solutions, such as upgrading customer relationship management systems, tightening third-party access controls and mandating encryption and multi-factor authentication measures.

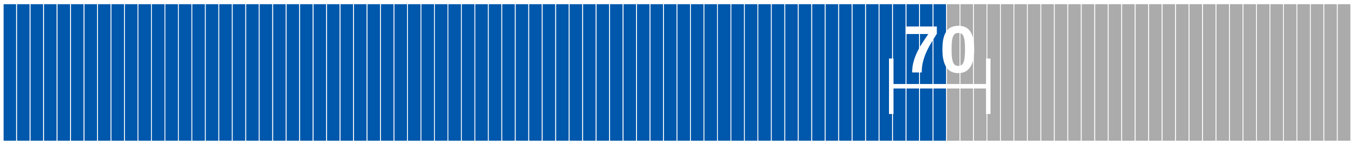
3. Reinforcing existing security protocols and policies to establish a more resilient defense against the ever-evolving cyber threat landscape confronting the sector.



Education

With the Education sector's growing dependency on digital learning environments and online resources, incidence of cyber threats has surged, making the protection of vast holdings of confidential data a pressing concern. Education entities, ripe with sensitive student and staff information, are prime targets for data breaches and phishing schemes. Despite an uplift from 68 (high mediocre) to 70 (low moderate) in their security culture score year over year, educational institutions still linger at the lower end in industry comparisons. The Compliance dimension saw an uptick by four points to 70, and Norms improved slightly by two points, indicating positive change. Nevertheless, the Responsibilities metric, having stayed low at 66 for consecutive years, reveals an ample opportunity for further progress. During 2023, schools, particularly at the K-12 level, were confronted by a wave of cyber attacks, with nearly 29% exploiting system vulnerabilities and about 30% instigated through phishing efforts. A notable incident was the MOVEit data breach, which compromised the records of approximately 900 schools and sensitive data pertaining to over 51,000 individuals, ranging from personal identification to educational details.

Additionally, the emergence of generative AI has become a focal point in the educational landscape. It's imperative for institutions to consider the effects of these tools on student learning and to communicate the ethical consequences connected to academic misconduct, including cheating and plagiarism. Various schools have already developed rules and guidelines aimed at preventing misuse of such tools while endorsing appropriate use to bolster research and learning.

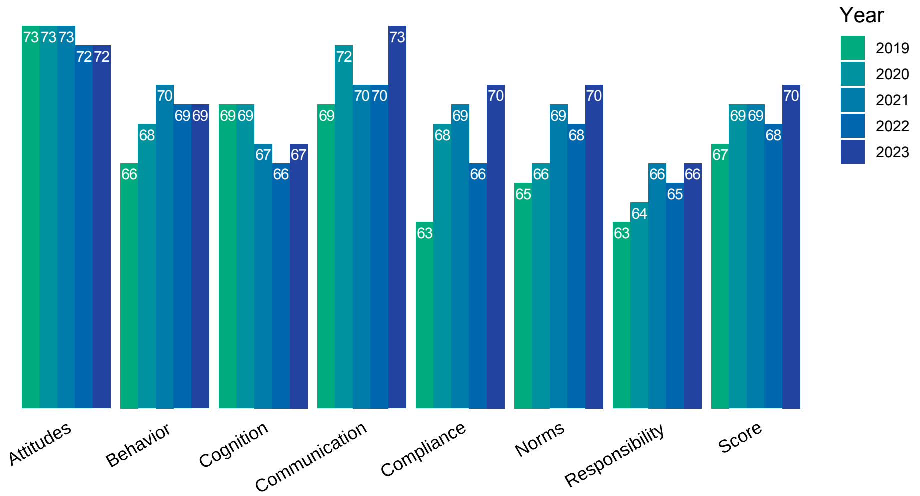


175

27,799

68 70

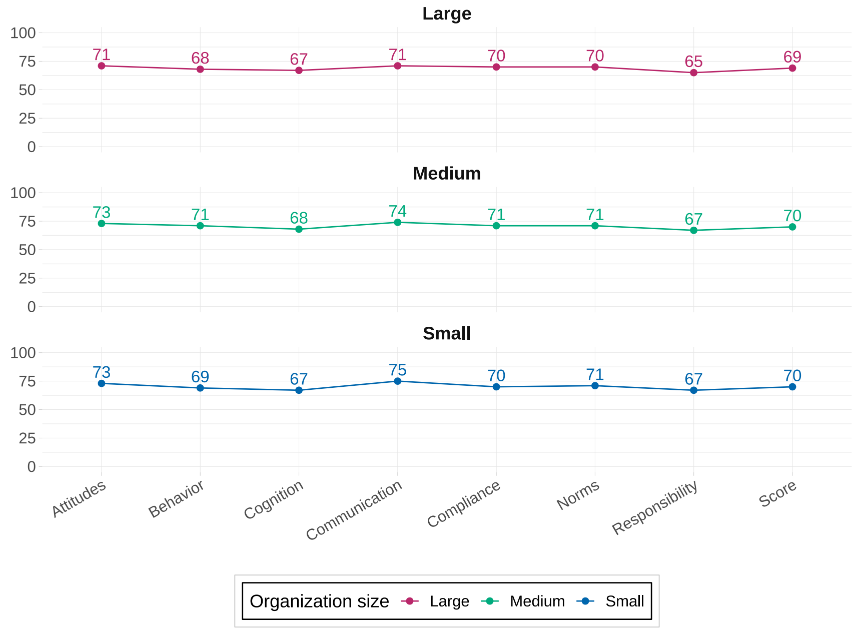
Security culture trends across all dimensions in Education



Areas for Improvement

To mitigate these risks, institutions must focus on strengthening their incident response protocols, bolstering staff cybersecurity training, educating students on cyber hygiene, enhancing their IT security systems and ensuring adherence to data privacy regulations. However, a critical issue to navigate is the perennially limited funding within public education settings. Limited funding curtails their ability to adequately invest in proactive cybersecurity measures. Improvements here could derive from regular security training and phishing simulations for staff, heightening their awareness of the pivotal role they play in thwarting cyber threats. Students should also be well-informed about the inherent dangers of online learning platforms. Moreover, ensuring an adequate allocation of resources, including budgeting for cutting-edge tools and comprehensive training, is key to cultivating an improved security culture score over time.

Education

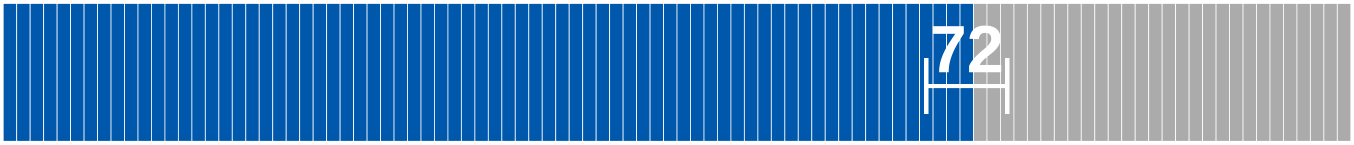


Energy & Utilities

The Energy & Utilities sector, with its intricate interconnection between physical and cyber infrastructure, holds a unique position of increased potential vulnerability to incursions by foreign intelligence entities and cybercriminals. Groups such as the U.S. Federal Government's Cybersecurity Risk Information Sharing Program (CRISP) serve as mechanisms of defense. For example, CRISP's continuous data collection via information sharing devices is aimed at identifying malicious actors within the sector. Moreover, an annual event, the Cyber Security for Energy and Utilities Conference—now in its fifth year—provides an essential platform for sharing critical information. While numerous organizations exist to provide this type of support, the industry's security culture score has shown a modest increase, standing at 72 (low moderate) in the most recent survey.

According to a report on cyber attacks on Vital infrastructure, a substantial 60% of these attacks are orchestrated by state-affiliated agents. Furthermore, internal staff inadvertently enable nearly 33% of these attacks. The energy sector is a primary target for threat actors, attracting 39% of attacks, a figure more than triple the attack volume in other sectors like critical manufacturing (11%) and transportation (10%). This research also underscores the urgency to bolster IT system security as a key strategy for countering cyber attacks on critical infrastructure and manufacturing facilities.

Indeed, over 80% of Operational Technology (OT)/Industrial Control System (ICS) incidents analyzed were triggered by a compromise of an IT system. The report attributes this predominance of IT system compromise to the escalating interconnectivity between IT and OT frameworks and applications. Phishing remains the primary mode of attack, accounting for 34% of methods used. This finding highlights the pressing need for robust cybersecurity measures such as segmentation, air gapping, zero trust and security awareness training to curtail risk. Although over 80% of threat actors originate from outside the organization, insiders who unintentionally fulfill a facilitative role feature in approximately one-third of incidents.

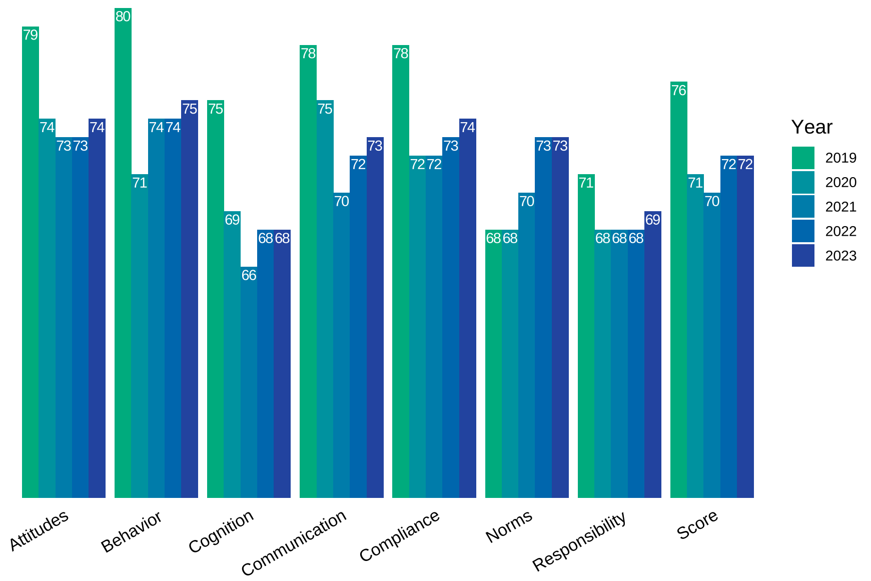


191

46,604

72 → 72

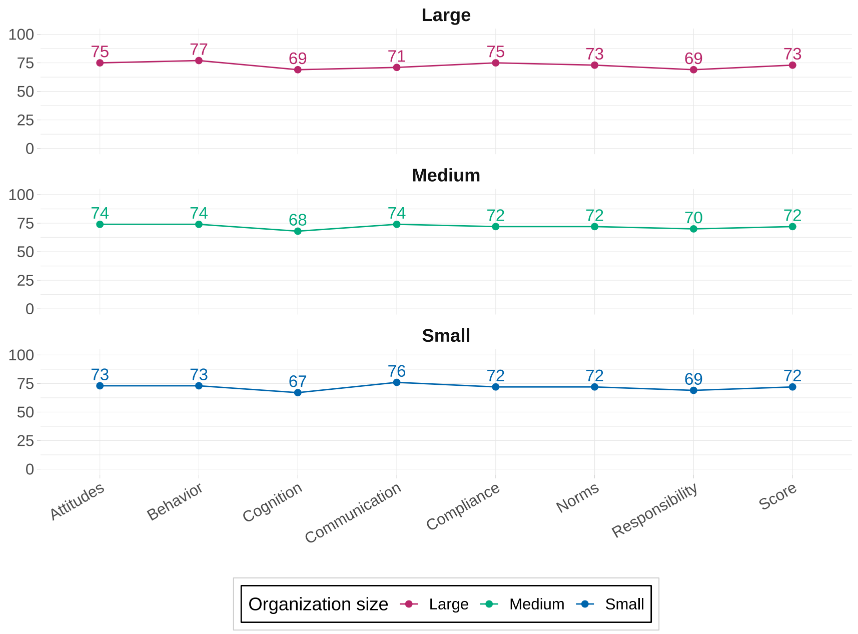
Security culture trends across all dimensions in Energy & Utilities



Areas for Improvement

The persistent threat of phishing attacks on the Energy & Utilities sector, as highlighted by industry reports, emphasizes the urgency of bolstering cybersecurity measures. Despite a consistent Cognition rating of 68 and a marginal improvement in Responsibilities, now at a score of 69, these figures mask the pressing need for comprehensive employee vigilance. Merely offering training sessions is insufficient. It is vital for employees to receive ongoing practice in identifying and responding to potential threats. A strategy that integrates continuous learning and consistent testing will significantly enhance the sector's defense capabilities against such cyber attacks.

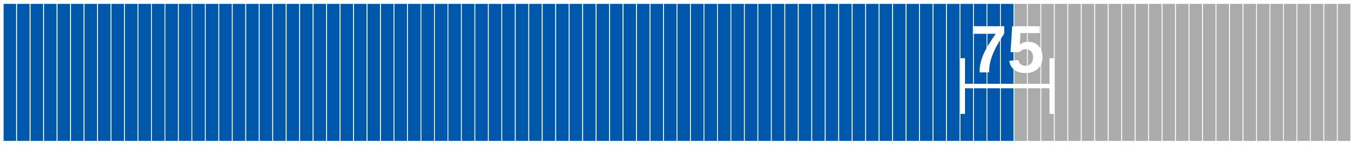
Energy & Utilities



Financial Services

Investors and lenders are approaching their operations with heightened caution, leveraging technological advances to mitigate risks, optimize expenses and enhance productivity—all while prioritizing a seamless customer and employee experience. These dynamics significantly influence the emerging trends in Financial Services for 2023. The overall security culture score had a one-point drop to a mid moderate 75. However, the landscape is becoming increasingly challenging due to weakening economic output, rising interest rates, and heightened international political tensions, amplifying difficulties for banks, insurers and fund managers. The outlook for new financial challengers, including fintech and cryptocurrency entities, appears to be even more formidable.

Financial institutions face a substantial threat from cyber attacks, with an average loss of approximately $5.9 million per data breach, surpassing the global average by 28%. Regulatory concerns further shape how financial companies respond to these threats and allocate resources to reduce overall risk. While 48% of financial attacks originate from malicious actors, human error accounts for 33%. The primary attack vectors include phishing (16%) and compromised credentials (15%). Successful breaches often grant attackers access to millions of transaction and client records, with the average cost for breaches that involve at least 50 million records exceeding $300 million. Despite these challenges, there is positive news. Finance organizations demonstrate a proactive approach in detecting and containing data breaches, surpassing global averages. While companies worldwide take 204 days to identify and 73 days to contain a breach, the financial industry achieves these milestones in 177 and 56 days, respectively. In 2023, 39% of financial organizations reported extensive use of security AI and automation, reflecting a commitment to swiftly and effectively addressing cybersecurity risks.

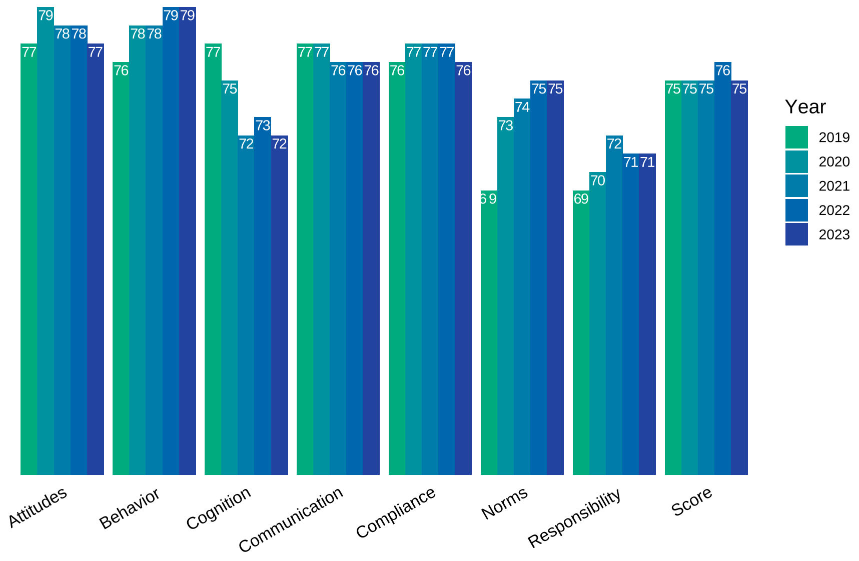


76 75

420

47,227

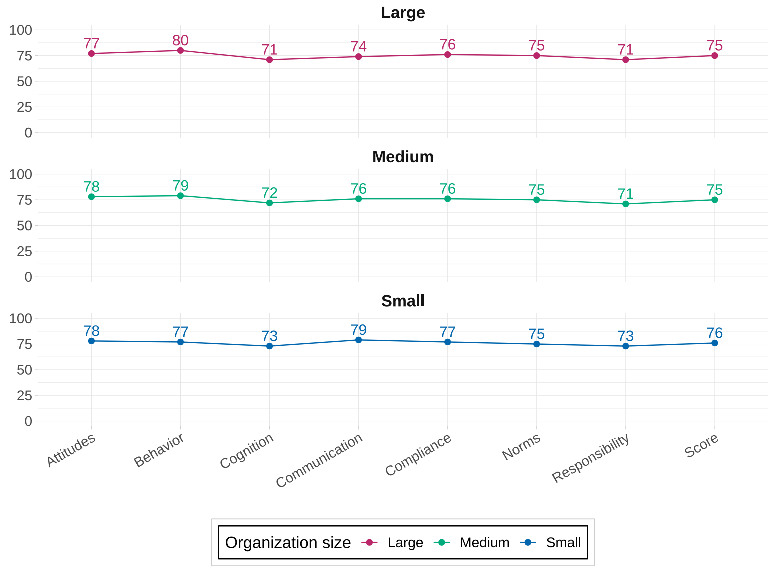
Security culture trends across all dimensions in Financial Services



Areas for Improvement

Industry reports have brought to light the ongoing vulnerability of the financial services sector to phishing attacks, underlining the critical need for stronger cybersecurity defenses. The sector has experienced a slight decline in its overall score, having dropped by one point since last year, with individual dimensions of Attitudes, Cognition and Compliance each losing a point, now standing at 77, 72 and 76, respectively. Furthermore, the persistently low score in the Responsibility dimension, which currently sits at 71—a marginal improvement from 2022's peak of 72—underscores the urgent call for heightened employee alertness. Simply providing training sessions is no longer adequate. Instead, employees must be immersed in continuous and practical learning experiences designed to sharpen their skills in detecting and neutralizing potential threats. The adoption of a holistic strategy encompassing relentless education and regular assessments will materially reinforce the sector's defenses against cyber threats.

Financial Services

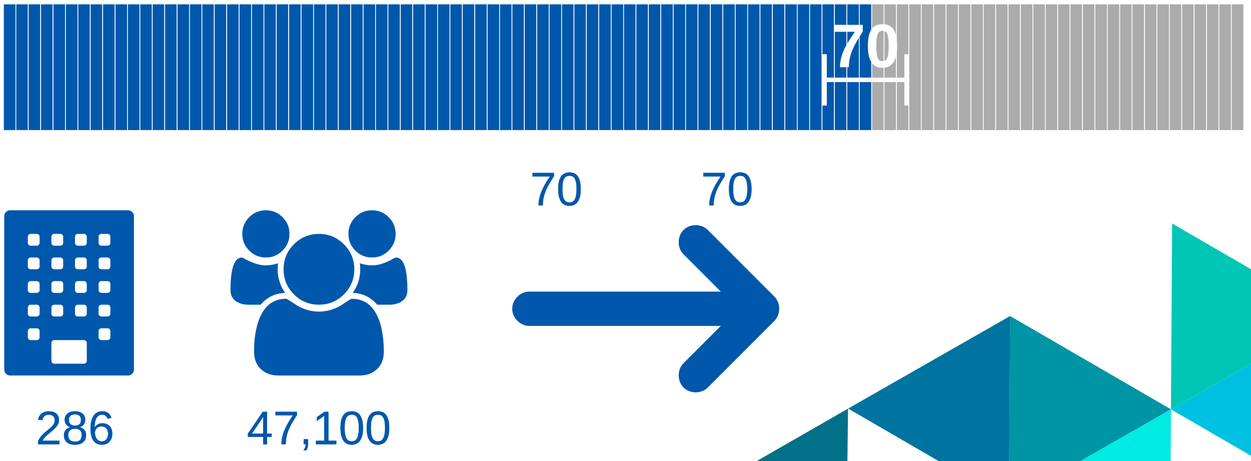


Government

In March 2023, the U.S. Federal Government unveiled its National Cybersecurity Strategy, charting a comprehensive course toward bolstering the nation's cyber defenses. Central to this strategy are two key objectives: requiring major public and private entities to shoulder a larger portion of cyber risk mitigation and reshaping the economic landscape to better reward long-term commitments to cybersecurity. This forward-looking strategy is structured around five synergistic pillars aimed at fortifying critical infrastructure, neutralizing cyber adversaries, incentivizing market-driven security enhancements, investing in future-proof digital systems, and cultivating international alliances for cooperative cyber defense.

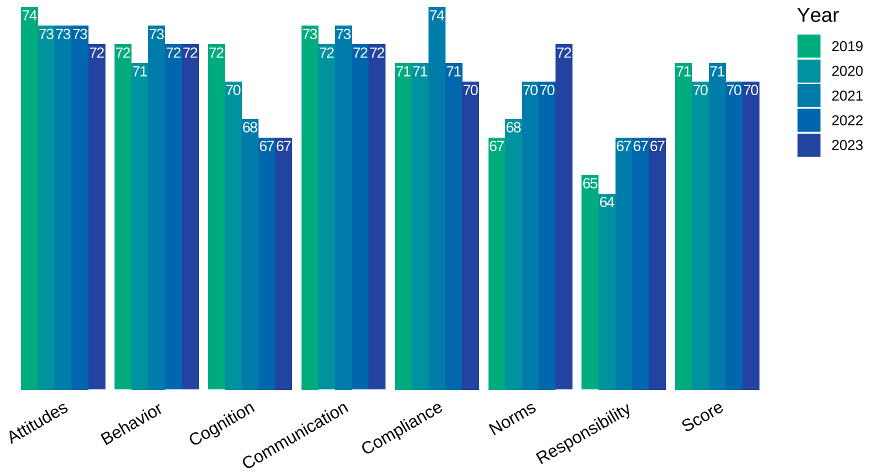
While the strategy sets an aspirational roadmap for a more secure cyberspace, the accompanying implementation details vital for a full appraisal of the plan's feasibility—such as agency responsibilities, legislative needs and initiative leadership—were not disclosed alongside the National Cybersecurity Strategy (NCS). Adding to the urgency for detailed action plans, the strategy's release comes at a time when the sector continues to face challenges, as reflected in an underwhelming security culture score of a low moderate 70. This underscores the crucial need for precise, actionable measures to effectively operationalize the strategy's five pillars and ensure a robust cyber posture for the United States.

Cyber threats to governmental infrastructure, fueled by nation-state actors and profit-seeking hackers, continued to pose critical challenges in 2023, as underscored by several high-profile incidents. Notably, Microsoft unearthed a Chinese cyber-espionage operation, attributed to the Storm-0558 group, which had infiltrated customer email accounts since May 15, 2023. Targets included personnel within the U.S. State and Commerce Departments along with other federal entities, hinting at a deeply concerning security lapse. This breach came to light after attackers successfully seized control of a Microsoft engineer's work account, which precipitated severe criticism and allegations of carelessness from a U.S. legislator directed toward the corporation. Further, in a troubling revelation in August 2023, The UK's Electoral Commission announced it had fallen prey to a "sophisticated cyber-attack." The incident compromised personal details of the UK's electorate registered from 2014 to 2022. The intricacies of the attack, coupled with the fact that the culprits evaded detection for an extensive 15 months, pointed toward objectives that likely extended beyond immediate financial exploitation. This breach's severity was later compounded by reports that the Electoral Commission had suffered an automatic failure in a Cyber Essentials assessment, reflecting significant vulnerabilities in its security framework.



INDUSTRY BENCHMARK

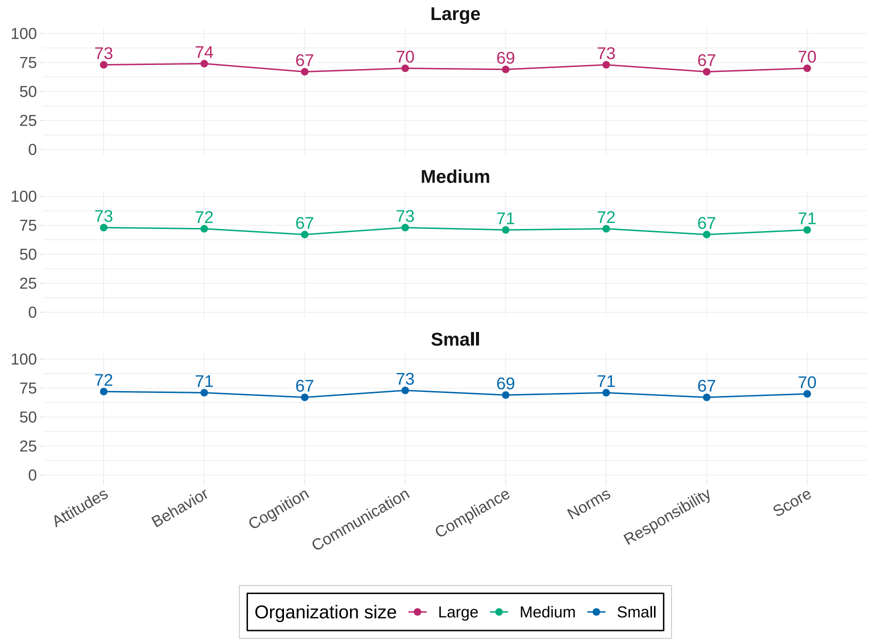
Security culture trends across all dimensions in Government



Areas for Improvement

Persistently low scores in Cognition and Responsibilities, both mirroring last year's mark of 67, are particularly worrisome. Furthermore, the slight drop in Attitudes and, more alarmingly, in Compliance by one point underscores the need for urgent action. These consistently subpar scores signal a pressing requirement for intensified security awareness training. It is imperative to not only bolster the workforce's knowledge but also to cultivate a deeper comprehension of the implications of their cyber habits on the overall security of the government. There's a clear necessity for enhanced training programs that underline the importance of understanding and internalizing an organization's implicit norms and ethical guidelines. This understanding, coupled with a strong sense of personal investment in safeguarding their organization, is vital to protect against threats from nation-states and independent hackers.

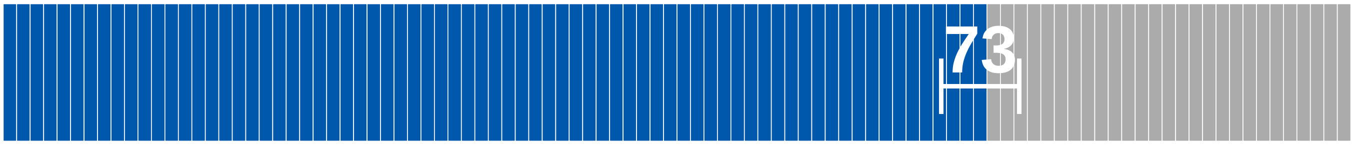
Government



Healthcare and Pharmaceuticals

The Healthcare and Pharmaceuticals sector has become increasingly aware of the importance of security culture due to the sensitivity of personal information and the presence of legal requirements such as the Health Insurance Portability and Accountability Act. The industry has responded to the need to protect sensitive information with continued adoption of telehealth and remote patient monitoring. However, this shift has also increased the need for the sector to be extra vigilant against cyber threats. Bad actors have capitalized on this opportunity and have begun to target remote workers as employees accessed corporate networks through personal devices. The Healthcare and Pharmaceuticals sector has a deep understanding of risk management, and this knowledge has helped employees respond to these new threats with mixed results. Overall, the sector has remained consistent in its performance with a score of low moderate 73, matching last year's results.

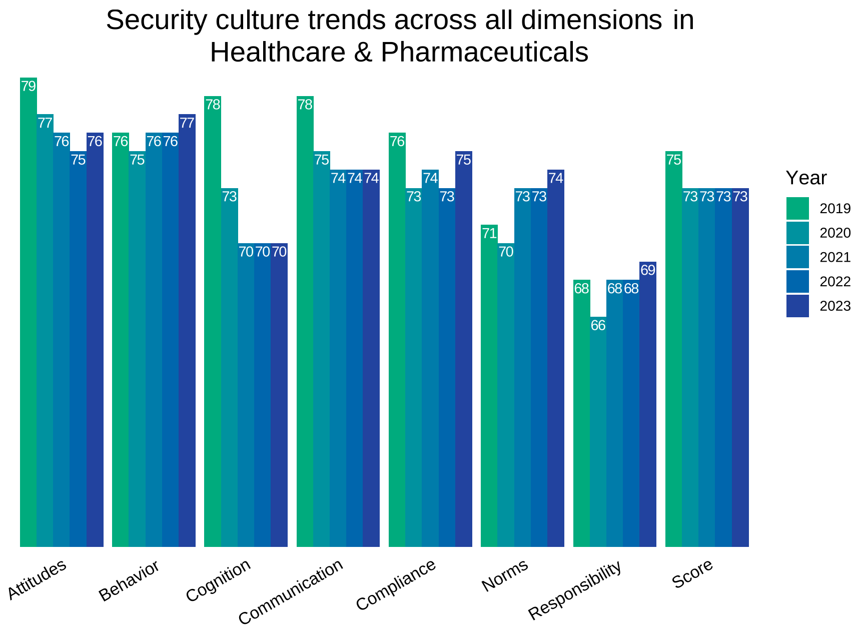
The IBM Cost of a Data Breach Report 2023 shows that the healthcare and pharmaceutical industries are among the most affected by data breaches, with these two sectors facing the highest average cost. This year has seen significant attacks on American healthcare organizations, with several prominent ransomware attacks making headlines. Notable examples include the data breach affecting 11 million patients at the for-profit HCA Healthcare, as well as the ransomware attack on Ardent Health Services, which led to the diversion of services at several hospitals. These health systems and hospitals have also been victimized by their vendors and contractors, underlining the broader vulnerability in this sector. In the pharmaceutical industry, the most common causes of data breaches are malicious attacks (45%), human error (28%) and IT failure (27%). Threat actors tend to favor phishing, compromised credentials and cloud misconfigurations when targeting these industries.



73 → 73

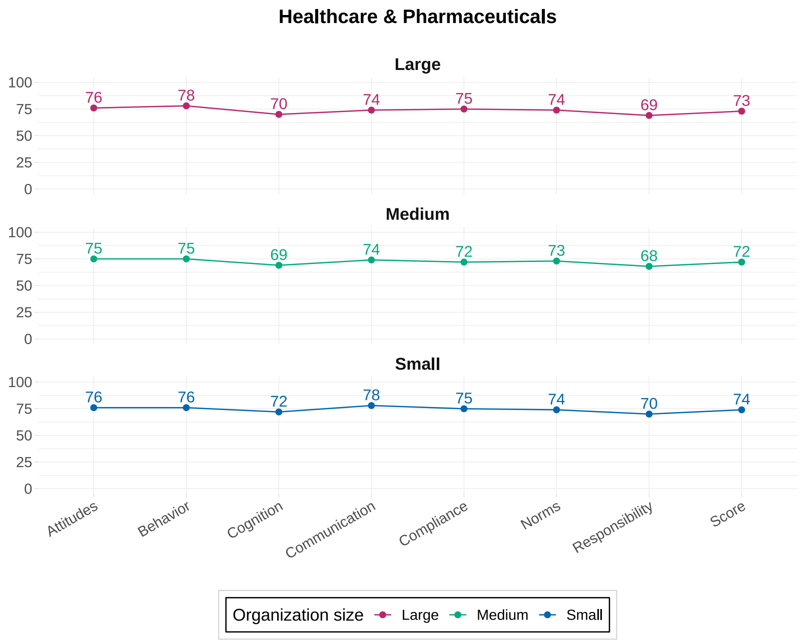
286

62,304



Areas for Improvement

The Healthcare and Pharmaceuticals sector showed promising improvement from last year's Security Culture Report findings. While the sector's scores in most dimensions remained consistent, there were notable enhancements in specific areas. The sector showed single-point improvements in Attitudes (76), Behaviors (77), Norms (74) and Responsibilities (69). Furthermore, there was a two-point increase in Comprehension (75), showcasing a rise in employee understanding of security matters. However, there's still room for significant improvement, particularly in the areas of Cognition (70) and Responsibilities, where employees could benefit from increased awareness and accountability. Overall, the report suggests that employees in the healthcare and pharmaceuticals sector are moving in the right direction in terms of security awareness, but there's still work to be done to reach a robust security culture.

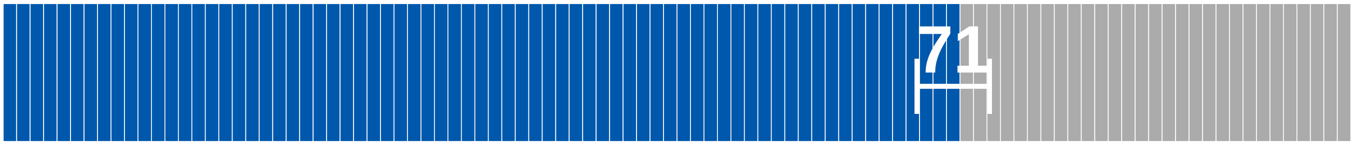


Hospitality

The Hospitality industry has come under increasing cyber threat, mainly due to its rich stores of sensitive customer data, heavy financial transaction traffic and sprawling IT networks. An industry assessment disclosed that nearly 31% of businesses in this sector reported at least one data security incident. Several factors exacerbate this cyber vulnerability—top among them are the high employee turnover rate, widespread use of public WiFi by customers and the sector's high-profile brand presence—making it an attractive prospect for cybercriminals looking to tap into data or monetary assets.

Amid a backdrop of cybersecurity pressures, the Hospitality sector has managed to nudge its security culture score upward from 70 to 71, still low-moderate, since the previous report. In this context, the Responsibilities dimension experienced a notable uptick, from 65 to 69, underscoring a growing sense of individual accountability. The Attitudes dimension saw an encouraging climb by three points, signifying a shift in mindset toward security concerns. Similarly, both the Cognition and Communication dimensions advanced by two points, although Cognition (68) and Responsibilities (69) still linger behind as the less favorably rated aspects within the sector's security posture. To further enhance the industry's security framework, leaders should champion comprehensive, continuous cybersecurity awareness initiatives that reach employees at all levels, underlining the criticality of cybersecurity as well as the collective responsibility each staff member holds in safeguarding the organization.

A case in point is the formidable cyber assault faced by MGM Resorts International in September 2023, when the company suffered a ransomware attack with financial repercussions surpassing $100 million. While this attack was particularly severe, the Hospitality sector generally reckons with a considerable cost of around $3.4 million on average for such breaches. As the sector increasingly adopts generative AI to refine guest experiences via automated chatbots and translation tools, it simultaneously raises the specter of additional data security concerns. The widespread advent of contactless payment technologies at dining venues and the confluence of smartphones with payment processing equipment also pave new potential paths for cybercriminal exploitation.

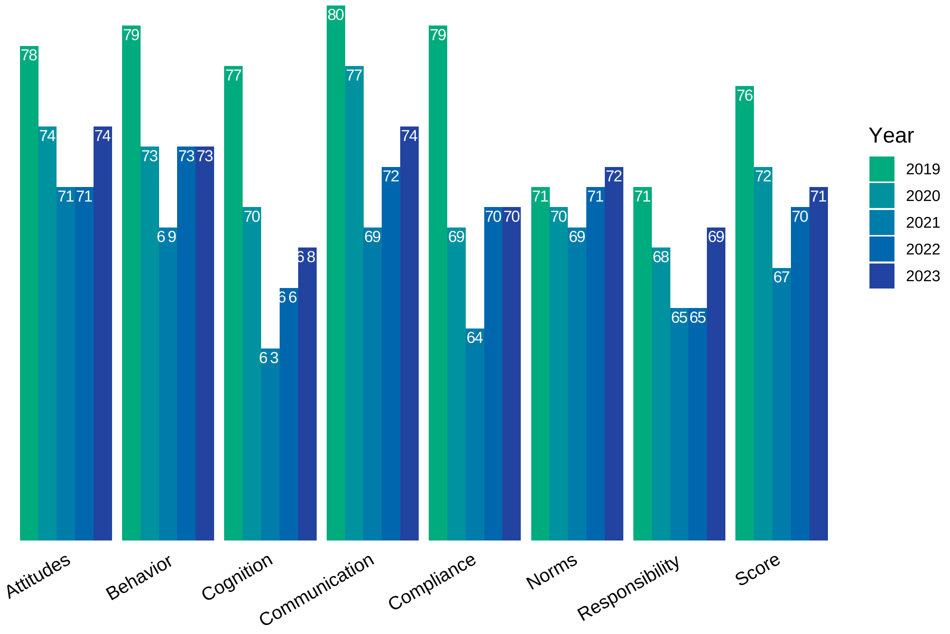


70 71

42

6,782

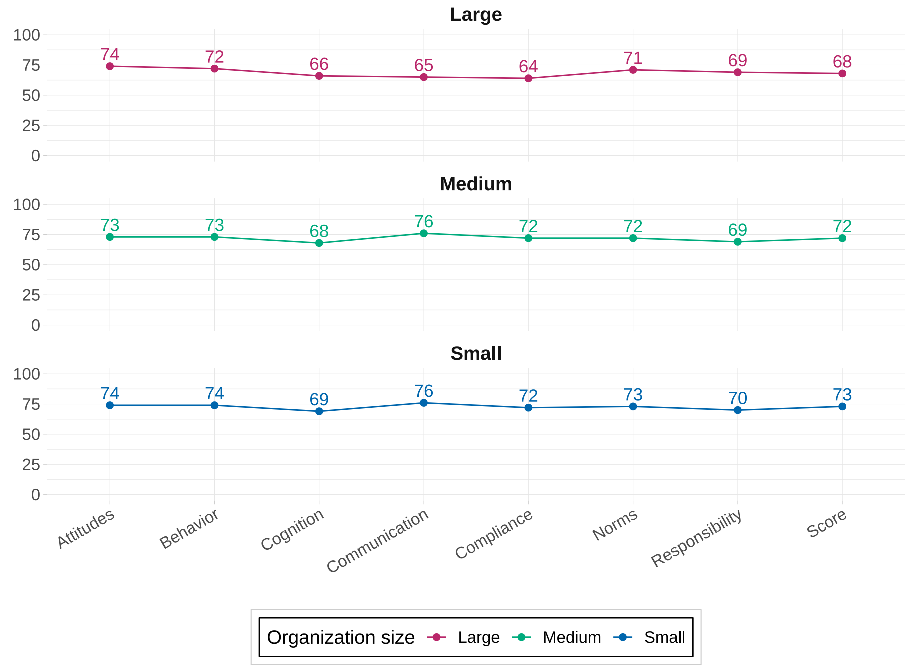
Security culture trends across all dimensions in Hospitality



Areas for Improvement

Industry leaders can strengthen their company's approach to cybersecurity by implementing continuous and comprehensive training programs for their workforce. These initiatives should emphasize the significance of cybersecurity, outline the potential risks and clarify the critical role each team member has in upholding the organization's digital security.

Hospitality

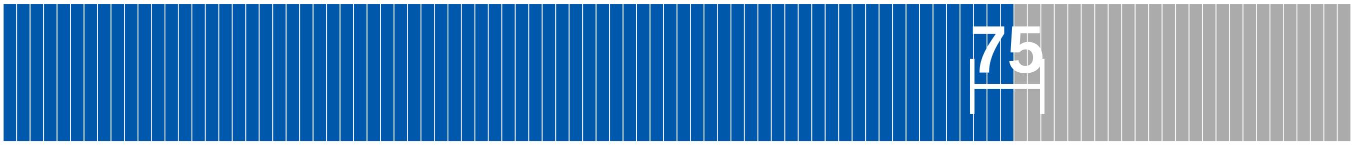


Insurance

The Insurance sector, scoring a mid-moderate 76 on the security culture score, experiences a significant ripple effect when subjected to a cyber attack, impacting not only the insurers themselves but also their clientele and all interconnected entities. Insurance companies hold vast stores of personally identifiable information (PII), along with policyholder details, financial data and medical records. These assets position them as prime targets for ransomware and other forms of cyber attacks. The sector operates under stringent regulations related to data privacy and collection. Concurrently, advancements in AI technology are enhancing accuracy and expediting processes, revolutionizing the sector by assisting in risk assessment, fraud detection and the minimization of human errors in administrative tasks. The infusion of AI is shifting the industry landscape through increased automation, claims optimization and more tailored customer engagement models.

The Insurance sector generally boasts some of the higher dimension scores in the Security Culture Index compared to other industries evaluated. With Behaviors (79), Attitudes (78) and Compliance (77) dimensions ranking high moderate, there is still room for growth in Cognition (72) and Responsibilities (71), which are at the low-moderate end. By helping employees draw clear links between their good intentions and their understanding of concrete actions toward enhancing organizational security, insurance companies can further fortify their cybersecurity posture.

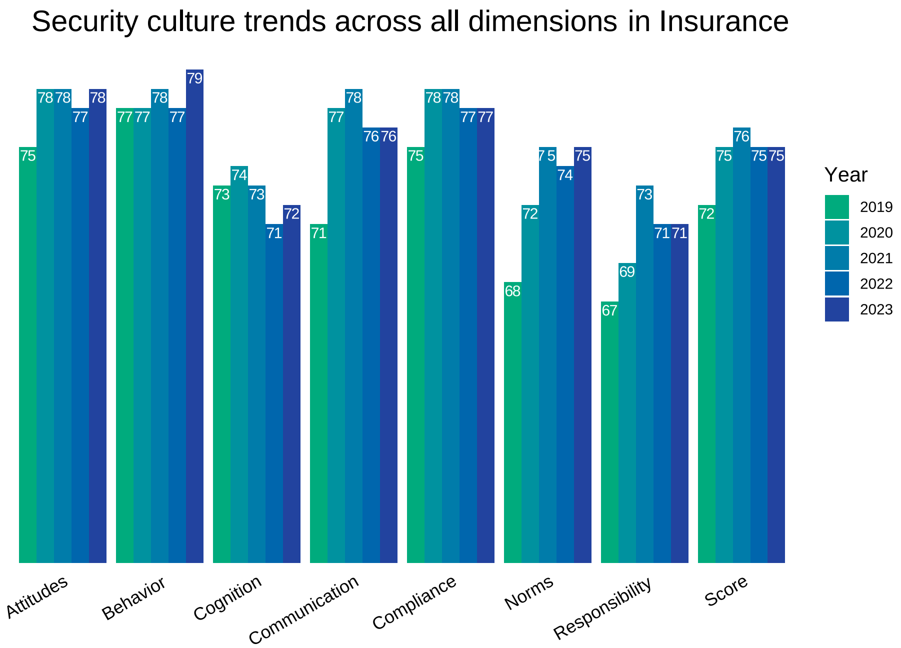
In 2023, the industry faced significant breaches, such as the ones at Sun Life and Genworth Financial, which affected thousands to millions of individuals. The trend seems persistent, with the Insurance sector identified as especially vulnerable according to KnowBe4's 2023 Phishing by Industry Benchmark Report. This ongoing susceptibility calls for insurance organizations to double down on engaging their workforce in security practices by emphasizing the importance of each individual's role in protecting the company's digital estate.



117

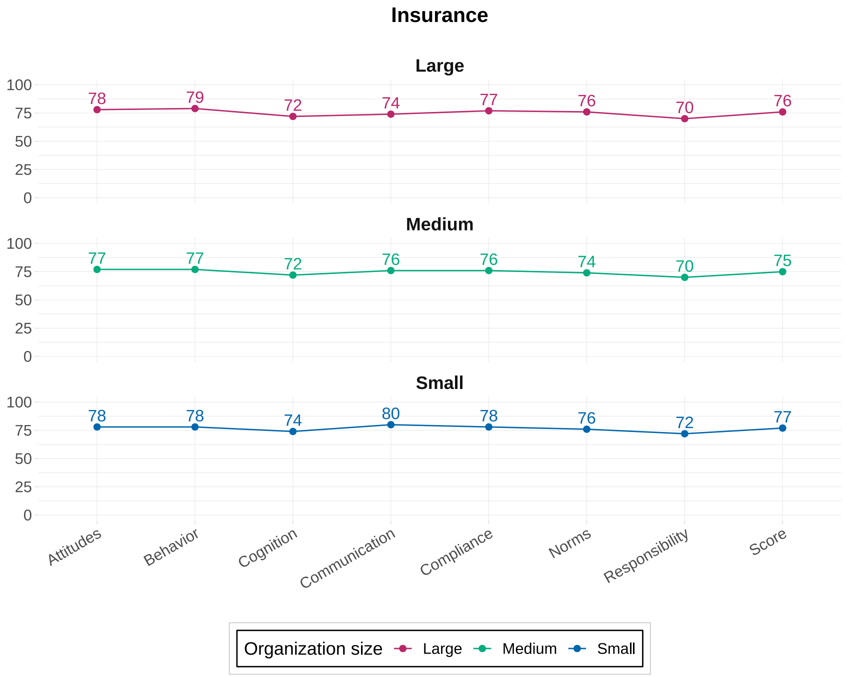
24,326

75 → 75



Areas for Improvement

In “**Transformational Security Awareness**,” Perry Carpenter highlights a crucial insight: awareness alone doesn’t equate to concern or action. He articulates that employees who lack an understanding of their organization’s security challenges may not realize their capacity to contribute to solutions, leading to indifference toward the overarching issue. It is essential to establish clear and relevant links between employees’ required actions and knowledge and the benefits that both the organization and the employees themselves will reap. By doing so, employees are more likely to embrace a sense of personal investment and responsibility in the security of their workplace.

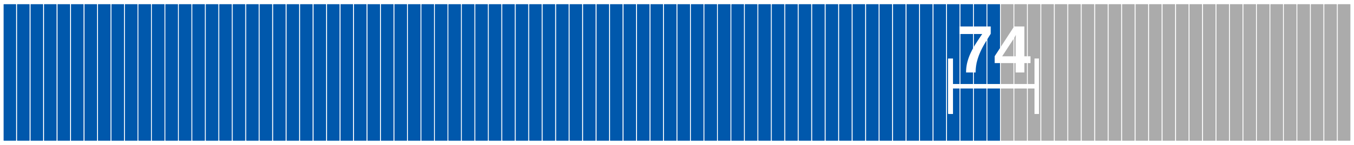


Legal

The Legal industry has maintained a steady security culture score of mid-moderate 74 compared to the previous year, showcasing no significant improvement. Given the high value placed on confidentiality in lawyer-client relationships, law firms have become a favored target for cybercriminals. Any breach can have dire consequences, such as reputational damage, financial repercussions and hefty legal penalties. Sensitive materials like personally identifiable information, criminal histories, medical and financial records and proprietary business data are abundant within these organizations. The inadvertent exposure of such confidential client data would be detrimental. To prevent such outcomes and avoid public disclosure, law firms are often inclined to pay ransoms demanded in cyber extortion cases. A report from Bloomberg Law cited a 2022 survey by the American Bar Association where more than a quarter of law firms acknowledged experiencing a data breach, an increase from the year prior.

In the scoring of specific security culture dimensions, the Legal sector performs well in Communication (77), Compliance (75) and Attitudes (75). Law firms, known for their strong communication skills, use this strength to ensure that everyone within the organization is informed and provided with necessary resources. Although employees are knowledgeable about policies and feel strongly about security concerns, there remains a disconnect when it comes to accepting personal Responsibilities (69) for the firm's overall protection. Security Week cited a breach affecting Orrick, Herrington & Sutcliffe, highlighting the challenges when over 600,000 individuals' data were compromised earlier in 2023 during a network intrusion. The repercussions of such breaches often lead to legal actions like class lawsuits.

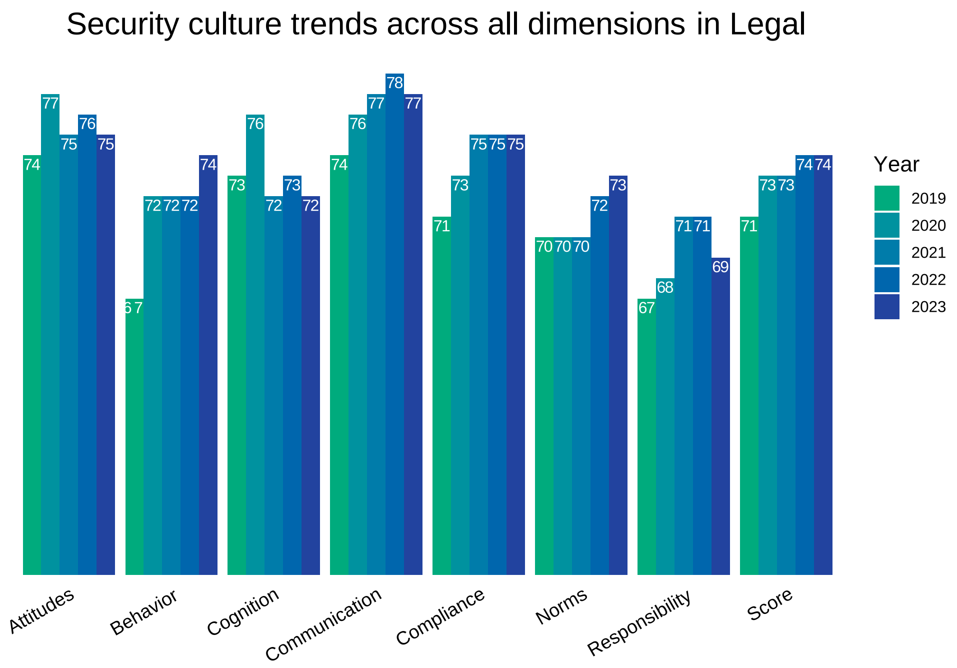
Additionally, advancements in AI technology are optimizing the way law firms review and process legal documents, conduct research across extensive case files and detect errors. These advancements promise considerable savings in time and resources while increasing precision in legal tasks. Also, AI-related errors can potentially cause hardships for clients. As AI evolves, its contributions to legal practice efficiency and accuracy are set to expand further.



76

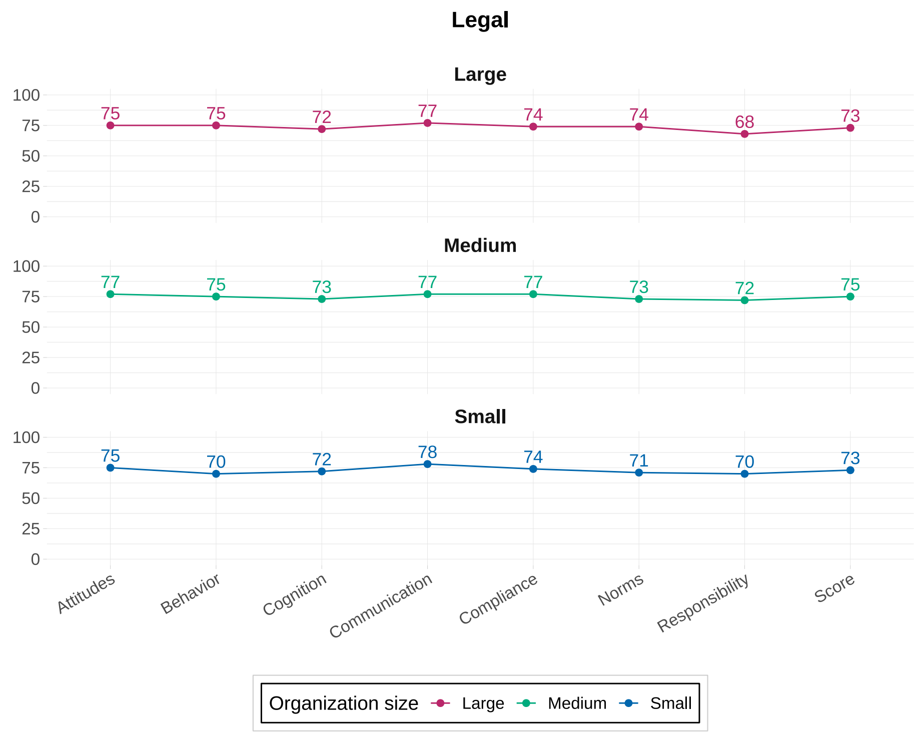
11,125

74 → 74



Areas for Improvement

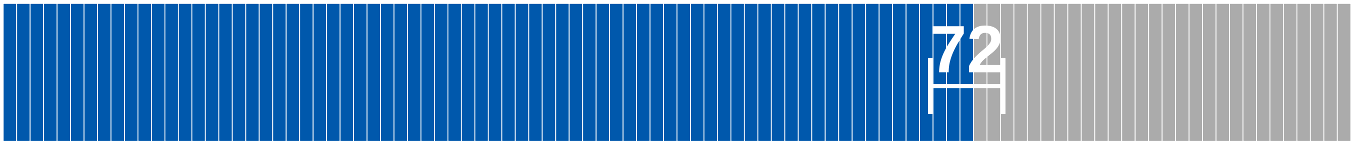
While employees might grasp and adhere to policy guidelines, it's crucial that they recognize their individual roles in safeguarding the firm and know how to actively apply their cybersecurity knowledge. The approach to security awareness and training shouldn't be confined to isolated sessions; rather, law firms should invest in ongoing, broad-based educational initiatives and rigorous exercises that address the vulnerabilities pertinent to the firm's digital ecosystem.



Manufacturing

The Manufacturing sector, with a modest increase to a security culture score of low moderate 72, represents a juicy target for cybercriminals. Incremental progress is hampered by reliance on outdated operating systems, disjointed security measures and a tendency to downplay the importance of regular security training. The sector often encompasses a diverse workforce with varying levels of cybersecurity preparedness. Despite these challenges, manufacturing firms tend to inadvertently offer cybercriminals multiple opportunities for entry—whether through customer interfaces or third-party vendor relationships—compounded by the elaborate and intertwined nature of supply chains. On a positive note, advancements in AI are becoming indispensable for manufacturers globally. Autonomous robotics and predictive analytics powered by machine learning are enhancing efficiency, boosting production and reducing environmental impact. These technologies are not replacing human workers so much as supplementing their capabilities, allowing for safer and more productive labor.

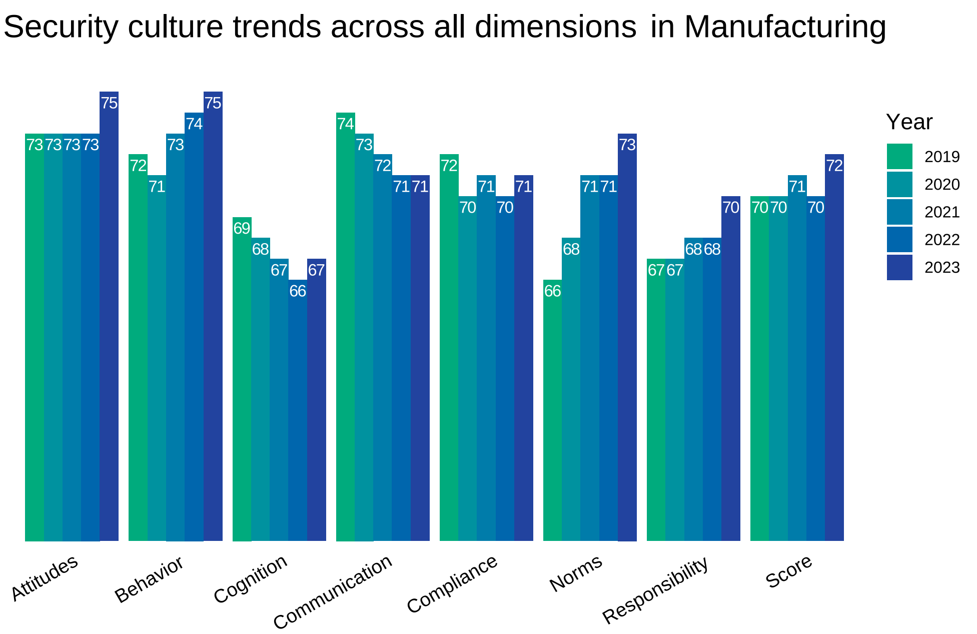
In the Security Culture Index, the Manufacturing sector achieved mid-moderate scores of 75 in both Attitudes and Behaviors. However, other dimensions remain lower, with Cognition notably at a mediocre 67. While there is recognition among employees that they can contribute to organizational security, a gap in actionable know-how persists. A case in point is the ransomware attack on Applied Materials in February 2023, where a supplier inadvertently became the source of a breach affecting the semiconductor giant. This incident underscores the vulnerability of supply chains and the potential financial consequences, estimated at $250 million for the Applied Materials attack. Cybersecurity professionals highlight this concern, noting that cyber attacks may shift focus to less secure nodes in the supply chain, potentially leading to security breaches in manufacturing down the line.



453

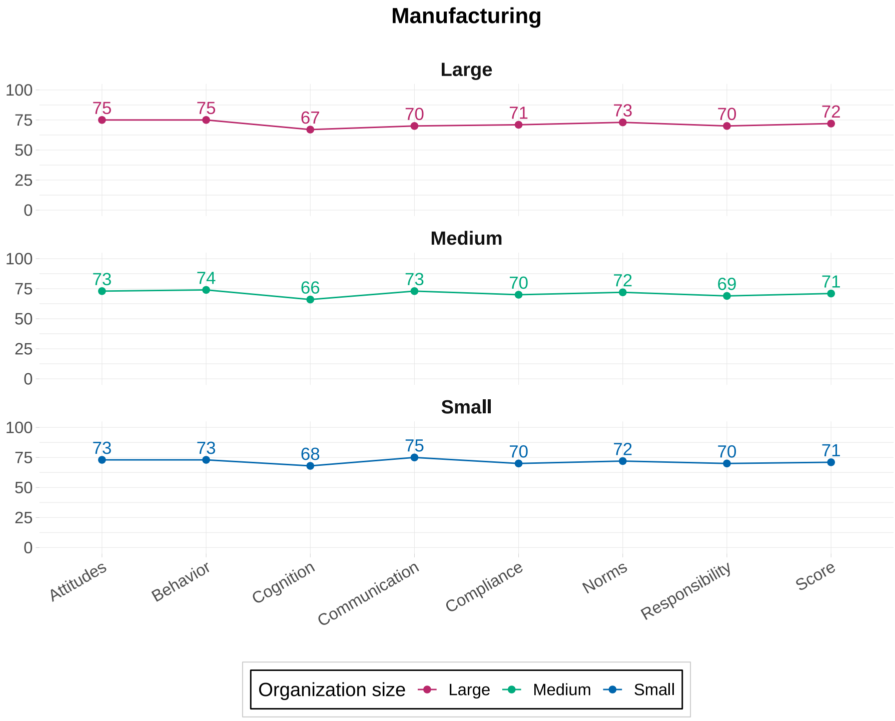
154,924

70 72



Areas for Improvement

Manufacturers must dedicate themselves to persistent and in-depth security training and assessment, extending to all staff tiers and employing a variety of communication methods to ensure that the information is compelling for various groups. To reinforce their digital defenses, they should conduct regular risk evaluations, conduct ongoing refinement of policies and controls and vigilantly oversee and limit access to data considered sensitive or confidential. These proactive measures are crucial for fortifying the sector's cyber infrastructure.



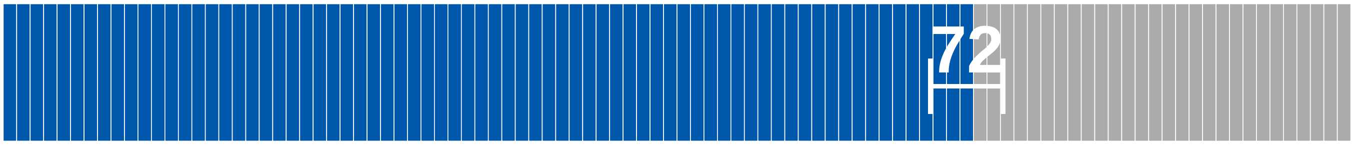
Nonprofit

The Nonprofit sector, with a security culture score of low moderate 72, is particularly vulnerable to cyber threats. Nonprofits frequently operate on tight budgets with lean teams and antiquated systems, leaving little financial leeway for investing in cybersecurity training or resources. There's a common misconception among such organizations that they aren't attractive targets for cybercriminals. However, the simplicity with which these entities can be exploited and the fact that attacks can be replicated across the sector make them potentially lucrative for attackers. Nonprofits house vast quantities of personal and financial information, making the stakes high. Any security slip-up can severely affect donations, partnerships and public trust. Moreover, these organizations often depend on outsourced services or part-time staff, which might widen security gaps, particularly regarding third-party access.

In March 2023, the case of Blackbaud, a cloud software provider for nonprofit entities, highlighted these challenges. The company incurred a $3 million SEC fine for not fully disclosing the extent of a 2020 ransomware attack, during which intruders obtained sensitive donor information. The nondisclosure of a ransom payment to secure a deletion promise from the culprits further complicated the issue.

Assessing Security Index Scores, most remain moderately low, except for Responsibilities; at 69, it tends toward the upper end of mediocrity. Dimension scores for Communication (75) and Attitudes (74) rank as the highest in the sector. This reveals a disconnect: while nonprofits communicate security practices and employees acknowledge the necessity of secure behavior, there appears to be a shortfall in empowering them to take proactive responsibility, often due to a lack of adequate tools, training and support.

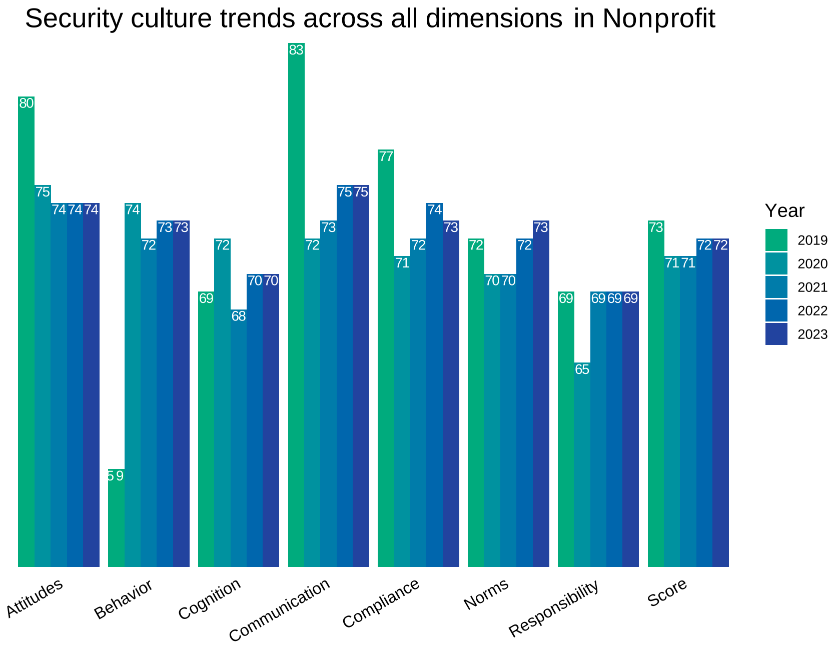
Yet, as AI technology progresses, it provides a silver lining for the Nonprofit sector. Innovations in AI can revolutionize fundraising and management, helping nonprofit employees refine donor engagement, screen potential contributors, forecast giving patterns, and more effectively pair volunteers to programs aligning with their experience and interests.



33

1,591

72 → 72



Areas for Improvement

Nonprofit organizations can enhance their cybersecurity posture significantly through practical measures that don't necessitate substantial monetary investments. Essential steps include:

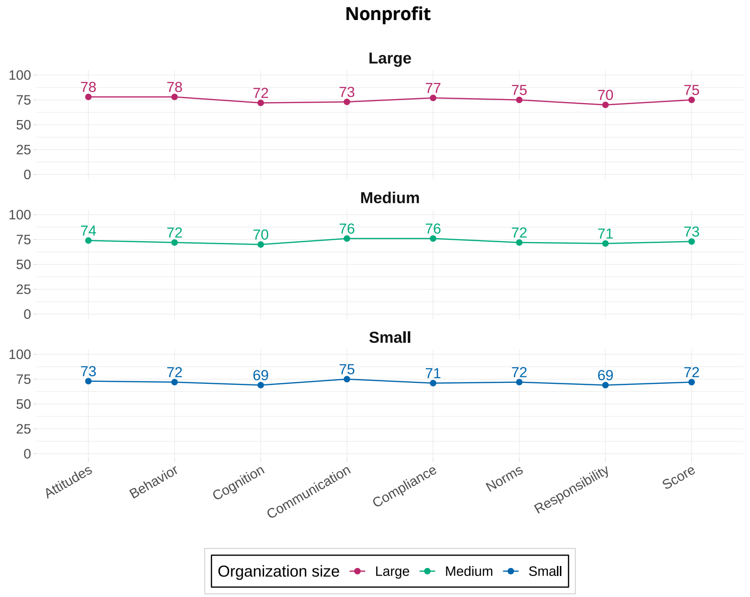
1. Implementing widespread and regular training programs to sharpen employee vigilance in recognizing and reporting suspicious communications and behavior

2. Enforcing frequent password changes and the adoption of multi-factor authentication to bolster account security

3. Restricting data access precisely aligned to each individual's role and duties within the organization

4. Diligently backing up all data at regular intervals to mitigate the impact of potential data loss incidents

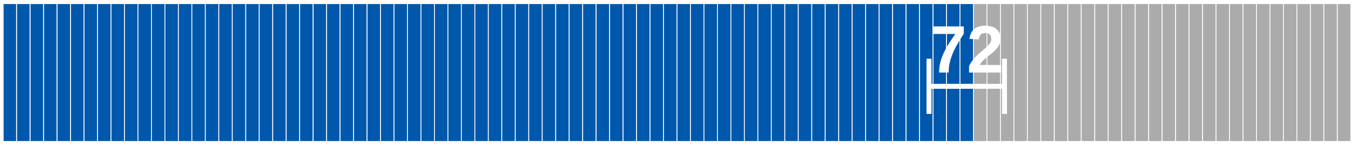
Fortunately, there are a plethora of training options available at no cost, providing accessible and manageable resources for strengthening Nonprofit cybersecurity readiness.



Retail and Wholesale

In 2023, the Retail and Wholesale sector nudged its security culture score up by a point to a low-moderate 72. The face of retail has been transforming, steadily moving away from the familiar in-store experience toward an era dominated by digital commerce. Online shopping is more popular than ever, providing consumers across the board with unprecedented variety and convenience, whether it's through direct home delivery, curbside pickup, or local courier services. Payment methods, too, have diversified beyond traditional channels, embracing tap-to-pay systems, cash apps like Venmo and Zelle, Apple Pay and even in-app purchases on social networks. These developments have dramatically simplified and reshaped consumer buying habits. Bolstered by AI, the Retail industry anticipates better customer segmentation, more streamlined operations, and the ability to refine pricing, forecasting and marketing strategies, as outlined by the National Retail Federation.

Despite an array of compliance obligations encompassing PCI DSS, SOX, HIPAA and several state-level privacy laws, retail operators continue to draw the attention of cybercriminals. Areas of vulnerability range from Point of Sale (POS) systems susceptible to intrusion to supply chain networks where vendors may inadvertently introduce malware into secure environments, providing criminals access to vast amounts of personal data and credit card information. Within the Security Culture Index, the Behaviors (75) and Attitudes (74) dimensions perform moderately well, yet Responsibilities (69) and Cognition (67) figures indicate a need for drastic improvement. This dichotomy suggests employees appreciate the importance of security and recognize the potential influence of their actions, yet lack complete understanding of the specific risks facing their sector. That appears to result in less personal ownership of cyber protective measures. A case highlighting these vulnerabilities comes from an MSSP Alert report in August 2023, where Dollar Tree suffered a data breach affecting some 2 million individuals, traced back to a compromised third-party service provider, Zeroed-In Technologies.

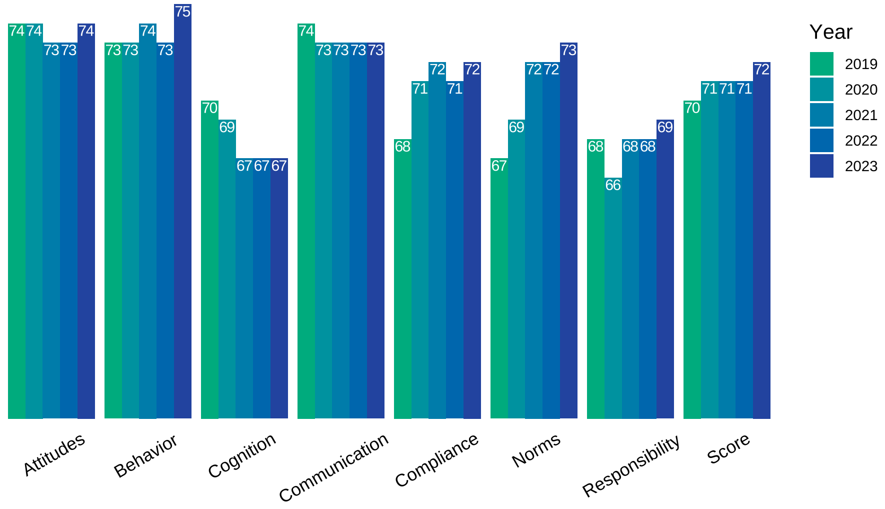


71 72

210

50,753

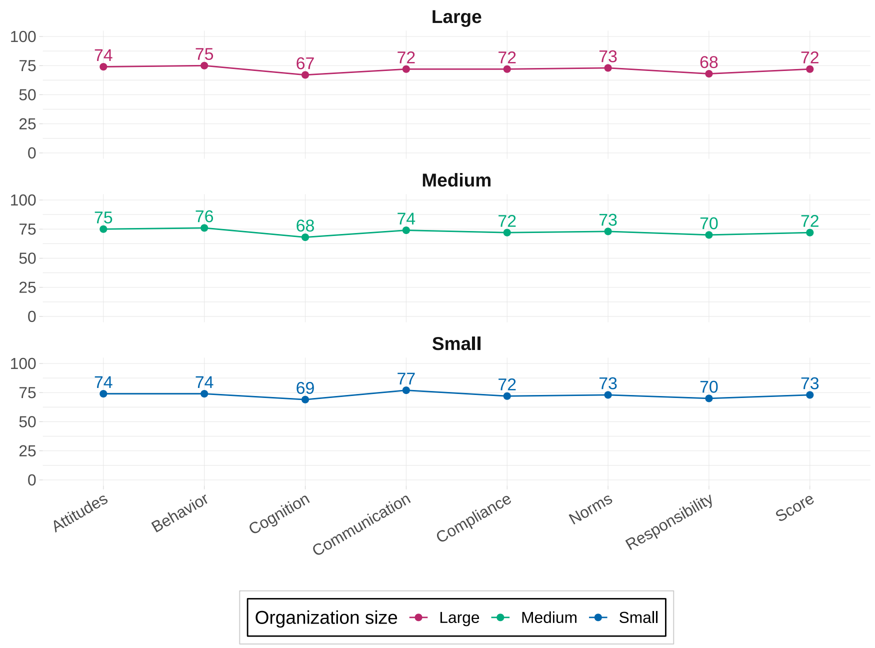
Security culture trends across all dimensions in Retail & Wholesale



Areas for Improvement

Retail and Wholesale businesses must acknowledge the complex network of vendor relationships that extend beyond their immediate partnerships, encompassing layers of subcontracted suppliers whose security measures might not be as transparent or robust. These successive layers of vendor relationships, which can often be several degrees removed from the primary entity, could harbor security weaknesses not immediately apparent to retail leaders. Developing a layered defense strategy that includes modernizing control systems and technologies (such as POS systems and advanced anti-fraud mechanisms), revising and reinforcing policies, authenticating customer data, as well as offering continuous, thorough staff training and assessment, will aid these businesses in pinpointing and monitoring potential vulnerabilities more effectively.

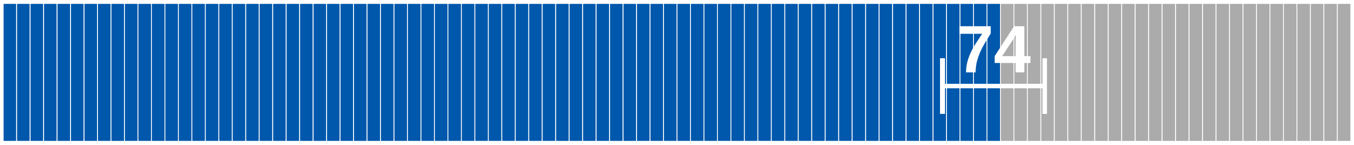
Retail & Wholesale



Technology

The Technology sector faces substantial headwinds as it deals with a tangle of challenges around supply lines, staffing and innovation, now complicated by the larger global economic situation and market uncertainty. The industry is being forced to adapt as consumers tighten their purse strings, product demand falls and market caps shrink. In response, they're streamlining their operations, automating with AI, and in some cases reconsidering inorganic growth through M&A. This sector's overall security score has decreased by two points since last year, down to 74. To improve their security culture, they will need to make significant additional efforts. The Technology sector's overall security culture score has experienced a concerning drop, from 76 to 74 (both mid moderate), with the exception of the Behaviors dimension (79 points), which remained consistent. The Cognition and Communication dimensions have particularly suffered a decrease, falling from 73 and 77 points to 71 and 75 points, respectively, in the current evaluation.

In 2023, data breaches have been a major concern for technology companies, particularly those that aim to protect customers from cyber threats. The year saw several notable breaches, including the MOVEit attacks, which exploited a vulnerability in Progress Software's file transfer product. The Russian-speaking hacker group Clop has been particularly active this year, targeting IT industry companies like IBM, Cognizant and Deloitte with data extortion attempts. The attacks on these companies are believed to be part of the larger MOVEit breaches that impacted over 2,000 organizations. In addition, other major cyber attacks have affected top IT channel players such as CDW and ScanSource, as well as vendors with large partner bases like Barracuda and Cisco. These attacks have exploited vulnerabilities in some of the most widely used products, causing significant disruptions to business operations.

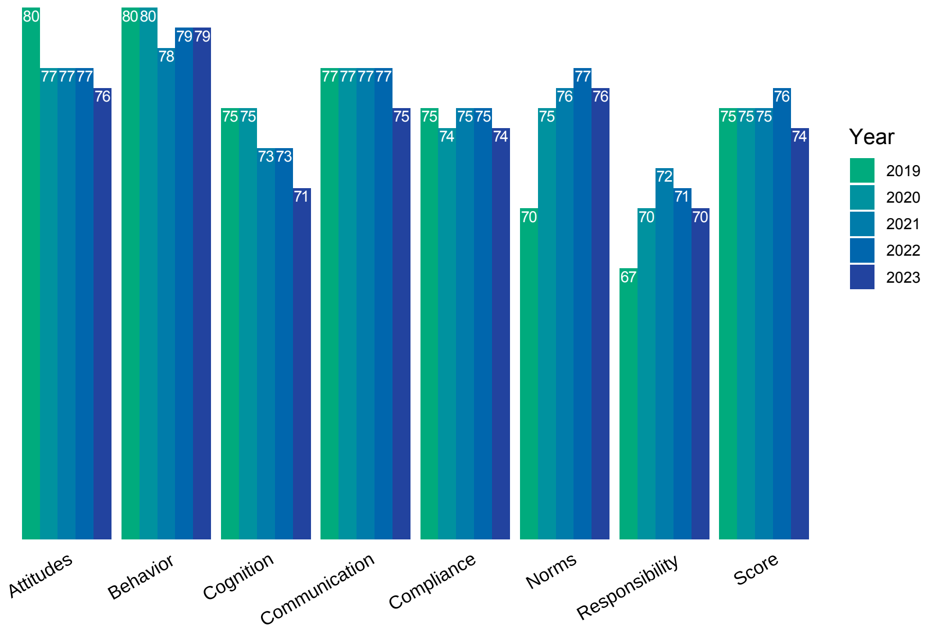


709

146,662

76 74

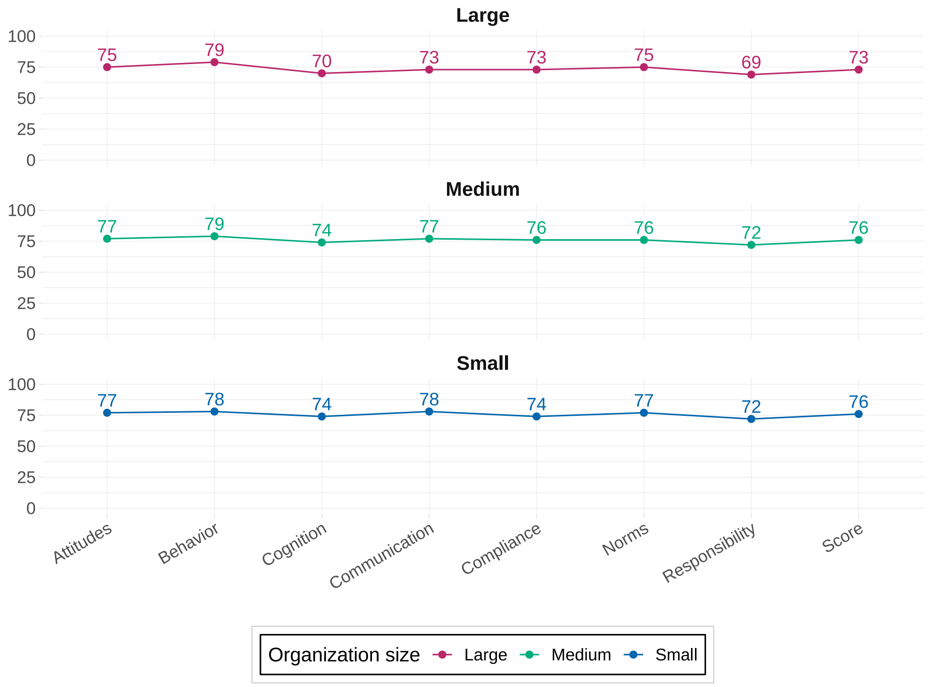
Security culture trends across all dimensions in Technology



Areas for Improvement

These tech trends may be attributed to the recent shifts in the technology sector's job market, which has resulted in a loss of seasoned professionals and their corresponding cyber hygiene practices. This loss could impact security culture until new hires can be adequately trained and contribute to a supportive corporate security culture.

Technology



Transportation

The Transportation sector is known to be cyclical. However, 2023 proved to be uniquely challenging for logistics companies. Though freight volumes and available capacity of the market ebb and flow predictably, multiple factors such as inflation, increased consumer credit usage and shifting consumer spending patterns away from goods and toward services are putting immense pressure on transportation companies. Despite these challenges, the Transportation sector maintains a consistent security culture score of low moderate 71, remaining unchanged from the previous year.

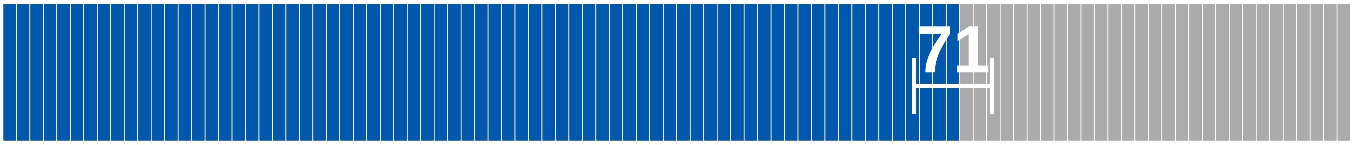
Trucking and logistics organizations have become a target for evolving cybersecurity threats as more operations rely on connected technologies. With the implementation of electronic logging and advanced features in newer fleet vehicles, the surface for cyber attacks has expanded significantly. As a result, transportation leaders are increasingly concerned about these growing risks. A recent Travelers Risk Index report found that 55% of respondents were worried about cyber attacks, with nearly 25% confirming their companies had already been victims of cyber crime. In recent months, high-profile attacks on Estes Express Lines and Orbcomm have highlighted the severity of the issue. Despite their traditionally simplistic technological infrastructure, the transition to digital operations has made transportation networks a more visible target for threat actors.

Areas for Improvement

The Transportation sector's security culture needs improvement. This year's survey results show a two-point drop in Responsibilities to 67 and a one-point drop in Behaviors to 74. This is in line with the previous iteration of this report, which identified a need for improvement across all aspects of their security culture. Taking a holistic approach and addressing all dimensions of security culture within the Transportation sector can help raise current issues and mitigate future ones. This approach should include:

1. Promoting personal responsibility: Educate employees on the importance of taking personal responsibility for their actions and how it relates to overall organizational security.

(Continued on next page)

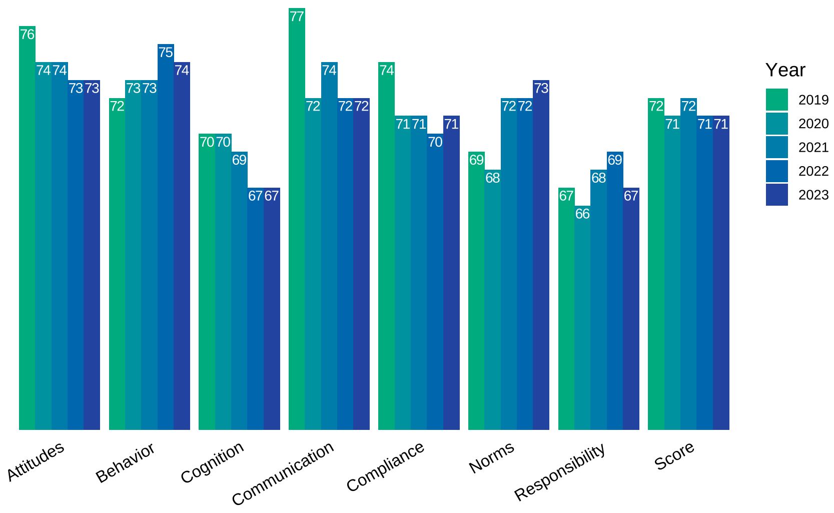


71 → 71

114

33,234

Security culture trends across all dimensions in Transportation



(Continued from previous page)

2. Model desired behaviors: Demonstrate positive behaviors that staff can emulate. Provide guidance on best practices for security and how these behaviors benefit the company and employees.

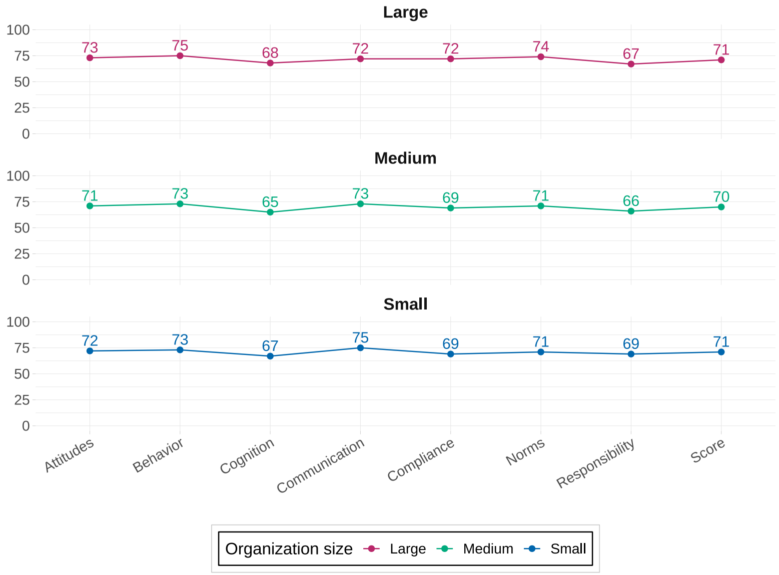
3. Encourage reporting: Ensure that staff feel comfortable reporting issues and potential breaches. Implement a system that allows for anonymity and protection from retaliation.

4. Address challenges in the physical and digital environment: Consider the unique challenges of the Transportation sector, such as managing a mobile workforce, and ensure that security policies and practices address these issues.

5. Provide adequate resources and training: Invest in employee training and resources to help them feel empowered in their role and to build confidence in their work.

By focusing on these areas and taking a comprehensive approach, the Transportation sector can improve its security culture and ensure that all employees are working toward maintaining a secure environment.

Transportation



Guidance for Improving Security Culture in Any Organization

By Joanna Huisman

While having a strategy is fundamental, formulating the appropriate plan with the most effective actions is paramount for achieving desired outcomes. KnowBe4 Research suggests a framework for understanding cultural transformation, encapsulated in the ABC's: **Awareness, Behavior and Culture**. This approach emphasizes a progressive journey from cultivating awareness to inspiring behavioral changes, which ultimately converge to shape and enhance organizational culture.

Understanding can shape actions and modifying actions can catalyze a shift in cultural norms. This logical sequence should be kept in mind while devising a roadmap for enhancing cultural ethos. Although mere awareness may not directly result in altered behaviors, it can serve as a potent mechanism for influencing them when presented in a content that resonates. Similarly, while transformation of an individual's behavior might not be synonymous with cultural transformation, the collective behavioral change of a group indeed signifies a cultural evolution.

To enhance the clarity and impact of the cultural transformation, a clear structure needs to be implemented. As detailed in the comprehensive KnowBe4 whitepaper titled "The Security Culture How-to Guide: Seven Steps to Improve Your Organization's Security Culture," outlined below are the seven fundamental stages in the continuous enhancement cycle in order to start on your security culture transformation.

Choose Two or Three Behaviors You Would Like to Change

Focus on behavior selection by pinpointing two or three high-risk behaviors that warrant attention and use KnowBe4's Security Culture Survey to gauge the current stance and establish a clear starting point. Now is the moment for precision and focus; it's essential to carefully curate your actions to ensure they are directly aligned with the overall organizational goals and specifically the results you aim to achieve. This is not the time to try and tackle everything at once, be selective.

Design a Plan to Influence Behaviors on an Organizational Scale

Behavior change can be effectively orchestrated through formal mechanisms such as establishment or modification of policies, or it can be cultivated through informal and social channels, frequently involving leaders or champions modeling the desired behaviors in a concerted effort to guide the workforce.

Engage in strategic plan development, where you will set feasible schedules for the intended behavioral interventions and appoint enthusiastic organizational champions who will advocate for these changes. Security Champions ensure communications are presented in clear, accessible language tailored to the specific needs of each country or department and are easy to comprehend. Recognizing diversity in communication preferences, it's crucial to tailor information delivery to align as closely as possible with each segment's preferred method of receiving messages.

Get Leadership Buy-In

Ensure leadership engagement by preparing a concise executive summary that outlines the objectives and secures backing of the organization's decision-makers. Solidify their support with a formal commitment to the action items set forth. Without endorsement from the executive level, any plan risks faltering and becoming futile, as employee buy-in often hinges on the recognition that the initiative is backed by the business. Also, seeing leadership exemplify the expected behaviors reinforces their importance and encourages employees to follow.

Communicate

Communication is key in this step also. Devise an employee communication strategy that connects with employees on a personal level and seek collaboration from different departments to make sure the message is both seen and heard. Additionally, offer accessible support to address any employee feedback or concerns.

Execute the Plan

Moving on to implementation, outline explicit goals and success indicators, complete with a well-planned timeline, all the while keeping open lines of communication with both champions and the executive team, providing support wherever necessary.

Measure Results

For evaluation, a subsequent Security Culture Survey should be conducted to measure progress and analyze any shifts or changes in culture from the first survey conducted. These findings need to then be shared with leadership in a simple but comprehensive report.

Determine the Move Forward Strategy

Lastly, actively solicit input from key stakeholders and use this insight to refine strategies for the future. Regularly updating behavioral targets in response to evolving threats will ensure the organization remains proactive in its approach to cultivating a robust security culture. Keep in mind that cyber crime is a continually evolving threat that shows no signs of diminishing. Instead, it's escalating with each passing day, becoming increasingly complex and pervasive. You must remain vigilant, always ready to preemptively address shifts in the landscape. Flexibility is key and you should be prepared to adjust your course swiftly if the threat demands it.

The overall message is this: Avoid feeling daunted...begin the journey. These suggested steps provide a straightforward strategy for setting out on a path that yields long-term benefits in fortifying your organization's security and enhancing the preparedness of your workforce.

About the Report

KnowBe4 Research developed this report using the highest research standards. The report leverages anonymized data from KnowBe4's Security Culture Survey. The sample size represents 10,539 surveyed organizations around the world, with more than 1,822,748 employees across 18 industry sectors, effectively making this the largest report of its kind published to date. What follows is a description of the methods used to analyze the data, along with descriptive tables.

How Data Was Collected

The data for this report was collected using the Security Culture Survey, which is available to KnowBe4 customers via the Kevin Mitnick Security Awareness Training (KMSAT) platform. The Security Culture Survey was developed by CLTRe 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. The question set and methodology have been refined over several years. The data collection period was from 2019 to 2023 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.

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 fewer 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.

Data Size

The data consists of 1,895,344 employees and 11,128 organizations. For the trends analysis, the final sample after data cleaning consisted of 1,822,748 employees and 10,539 organizations that completed the Security Culture Survey. For the industry benchmarks for 2023, the final sample consisted of 816,733 employees and 4,078 organizations that completed the Security Culture Survey. Data was collected from 111 countries.

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.

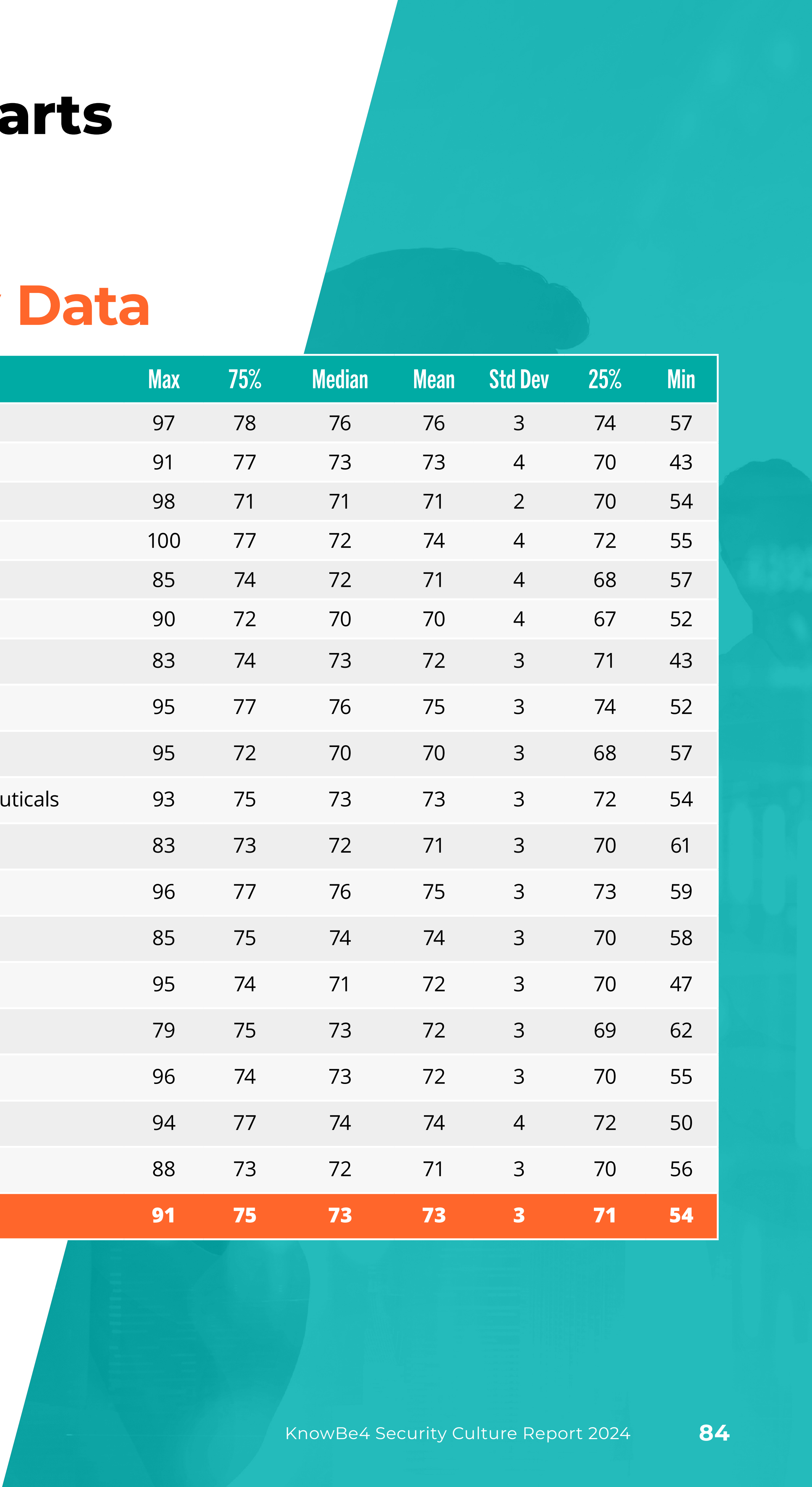
One of the benefits of aggregating scores to an organization level rather than at the employee level, is that the effects of organization size on industry benchmarks were neutralized. The unique algorithm for this transformation was designed by CLTRe and based on a complex conceptual understanding of organizational security culture.

Moreover, to enhance the accuracy and representativeness of our analysis, we implemented a data weighting strategy. After aggregating scores to the organizational level, the data was weighted to account for variations in organization size and response rates.

This was accomplished by assigning weights to each organization's score based on the number of valid responses it contributed. This weighting ensures that organizations with a larger number of responses have a proportionate influence on the overall results, preventing any single organization from skewing the industry benchmarks unduly. Additionally, for a global perspective, data was grouped by continent and further weighted by the number of organizations and employees in each group, ensuring accurate continental analysis.

Data Charts

Industry Data



Industry	Max	75%	Median	Mean	Std Dev	25%	Min
Banking	97	78	76	76	3	74	57
Business Services	91	77	73	73	4	70	43
Construction	98	71	71	71	2	70	54
Consulting	100	77	72	74	4	72	55
Consumer Services	85	74	72	71	4	68	57
Education	90	72	70	70	4	67	52
Energy & Utilities	83	74	73	72	3	71	43
Financial Services	95	77	76	75	3	74	52
Government	95	72	70	70	3	68	57
Healthcare & Pharmaceuticals	93	75	73	73	3	72	54
Hospitality	83	73	72	71	3	70	61
Insurance	96	77	76	75	3	73	59
Legal	85	75	74	74	3	70	58
Manufacturing	95	74	71	72	3	70	47
Not for Profit	79	75	73	72	3	69	62
Retail & Wholesale	96	74	73	72	3	70	55
Technology	94	77	74	74	4	72	50
Transportation	88	73	72	71	3	70	56
All	**91**	**75**	**73**	**73**	**3**	**71**	**54**

Descriptive Stats for Industry

Industry	Large	Medium	Small
Banking	76	75	76
Business Services	73	74	74
Construction	71	70	71
Consulting	73	75	75
Consumer Services	71	70	72
Education	69	70	70
Energy & Utilities	73	72	72
Financial Services	75	75	76
Government	70	71	70
Healthcare & Pharmaceuticals	73	72	74
Hospitality	68	72	73
Insurance	76	75	77
Legal	73	75	73
Manufacturing	72	71	71
Not for Profit	75	73	72
Retail & Wholesale	72	72	73
Technology	73	76	76
Transportation	71	70	71
All	**72**	**73**	**73**

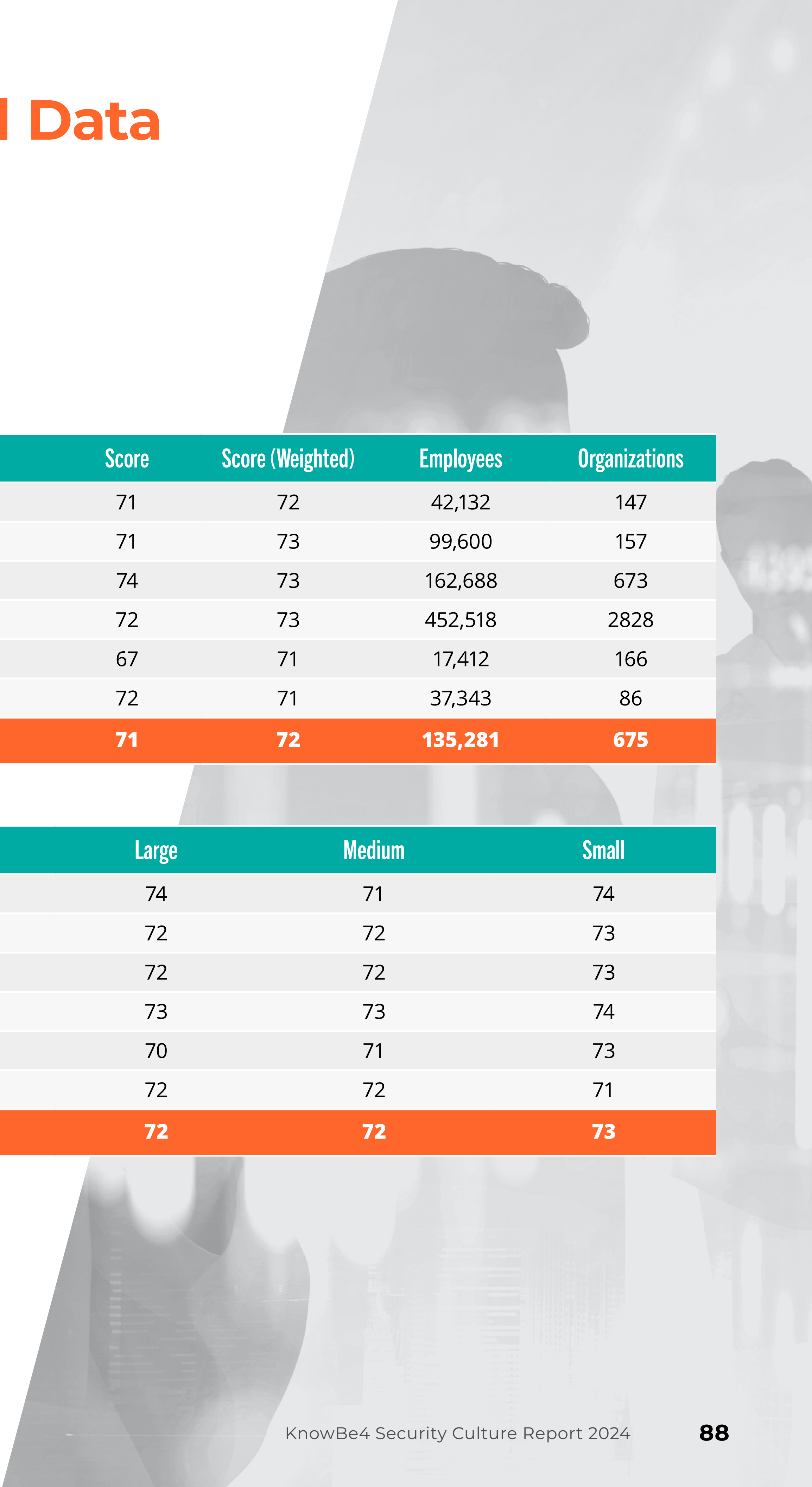
Industry	Employees	Organizations	Security Culture Score
Banking	43586	212	76
Business Services	49003	359	73
Construction	31238	126	71
Consulting	16795	144	74
Consumer Services	15680	125	71
Education	27799	175	70
Energy & Utilities	46604	191	72
Financial Services	47227	420	75
Government	47100	286	70
Healthcare & Pharmaceuticals	62304	286	73
Hospitality	6782	42	71
Insurance	24326	117	75
Legal	11125	76	74
Manufacturing	154924	453	72
Not for Profit	1591	33	72
Retail & Wholesale	50753	210	72
Technology	146662	709	74
Transportation	33234	114	71
All	**72**	**73**	**73**

Industry Data by Organization Size

Industry	Organizational Size	Attitudes	Behavior	Cognition	Communication	Compliance	Norms	Responsibility	Security Culture Score
Banking	Large	79	83	69	74	76	77	72	**76**
	Medium	77	79	70	75	76	75	72	**75**
	Small	78	77	73	78	78	74	72	**76**
Business Services	Large	74	76	68	73	71	74	70	**73**
	Medium	75	76	71	76	75	74	70	**74**
	Small	75	75	71	78	74	74	72	**74**
Construction	Large	72	73	66	72	72	72	67	**71**
	Medium	72	73	65	73	69	70	68	**70**
	Small	71	70	67	76	70	71	69	**71**
Consulting	Large	76	76	71	74	74	73	69	**73**
	Medium	77	77	74	76	76	75	72	**75**
	Small	75	76	72	78	74	75	71	**75**
Consumer Services	Large	73	74	67	72	70	71	68	**71**
	Medium	73	72	68	72	71	71	67	**70**
	Small	74	74	70	76	71	73	70	**72**
Education	Large	71	68	67	71	70	70	65	**69**
	Medium	73	71	68	74	71	71	67	**70**
	Small	73	69	67	75	70	71	67	**70**
Energy & Utilities	Large	75	77	69	71	75	73	69	**73**
	Medium	74	74	68	74	72	72	70	**72**
	Small	73	73	67	76	72	72	69	**72**
Financial Services	Large	77	80	71	74	76	75	71	**75**
	Medium	78	79	72	76	76	75	71	**75**
	Small	78	77	73	79	77	75	73	**76**
Government	Large	73	74	67	70	69	73	67	**70**
	Medium	73	72	67	73	71	72	67	**71**
	Small	72	71	67	73	69	71	67	**70**

Industry	Organizational Size	Attitudes	Behavior	Cognition	Communication	Compliance	Norms	Responsibility	Security Culture Score
Healthcare & Pharmaceuticals	Large	76	78	70	74	75	74	69	**73**
	Medium	75	75	69	74	72	73	68	**72**
	Small	76	76	72	78	75	74	70	**74**
Hospitality	Large	74	72	66	65	64	71	69	**68**
	Medium	73	73	68	76	72	72	69	**72**
	Small	74	74	69	76	72	73	70	**73**
Insurance	Large	78	79	72	74	77	76	70	**76**
	Medium	77	77	72	76	76	74	70	**75**
	Small	78	78	74	80	78	76	72	**77**
Legal	Large	75	75	72	77	74	74	68	**73**
	Medium	77	75	73	77	77	73	72	**75**
	Small	75	70	72	78	74	71	70	**73**
Manufacturing	Large	75	75	67	70	71	73	70	**72**
	Medium	73	74	66	73	70	72	69	**71**
	Small	73	73	68	75	70	72	70	**71**
Not for Profit	Large	78	78	72	73	77	75	70	**75**
	Medium	74	72	70	76	76	72	71	**73**
	Small	73	72	69	75	71	72	69	**72**
Retail & Wholesale	Large	74	75	67	72	72	73	68	**72**
	Medium	75	76	68	74	72	73	70	**72**
	Small	74	74	69	77	72	73	70	**73**
Technology	Large	75	79	70	73	73	75	69	**73**
	Medium	77	79	74	77	76	76	72	**76**
	Small	77	78	74	78	74	77	72	**76**
Transportation	Large	73	75	68	72	72	74	67	**71**
	Medium	71	73	65	73	69	71	66	**70**
	Small	72	73	67	75	69	71	69	**71**

Regional Data



Region	Score	Score (Weighted)	Employees	Organizations
Africa	71	72	42,132	147
Asia	71	73	99,600	157
Europe	74	73	162,688	673
North America	72	73	452,518	2828
Oceania	67	71	17,412	166
South America	72	71	37,343	86
All	**71**	**72**	**135,281**	**675**

Region	Large	Medium	Small
Africa	74	71	74
Asia	72	72	73
Europe	72	72	73
North America	73	73	74
Oceania	70	71	73
South America	72	72	71
All	**72**	**72**	**73**

Country Data

Country	Attitudes	Behavior	Cognition	Communication	Compliance	Norms	Responsibility	Security Culture Score
Angola	71	63	61	69	66	72	65	67
Burkina Faso	82	80	67	76	67	74	69	74
Botswana	75	75	65	71	67	72	74	71
Cameroon	79	77	57	67	57	70	76	69
Egypt	75	75	71	72	68	73	65	71
Ethiopia	77	77	71	75	74	72	71	74
Ghana	78	80	68	72	73	74	74	74
Kenya	78	80	71	75	77	73	75	76
Mozambique	67	63	59	73	58	67	65	64
Malawi	66	71	77	81	71	79	72	74
Namibia	76	77	66	69	70	74	71	72
Nigeria	78	82	71	73	74	74	76	75
Swaziland	78	66	65	74	64	68	73	70
Tanzania	70	69	60	76	63	67	64	67
Uganda	73	69	62	71	65	67	71	68
South Africa	75	75	68	74	70	74	69	72
Zimbabwe	74	68	66	78	69	70	75	71
Azerbaijan	72	60	64	73	65	63	65	66
Bahrain	70	67	67	74	66	71	63	68
Brunei	66	56	56	64	61	62	59	61
Cyprus	78	83	76	79	78	80	72	78
Georgia	77	76	79	79	74	75	69	76
Hong Kong	75	73	70	73	74	74	70	73
India	69	77	66	71	68	73	64	70
Indonesia	71	61	62	71	65	64	62	65
Israel	75	77	72	78	71	76	70	74
Japan	79	77	68	70	71	77	76	74
Jordan	78	81	74	79	77	79	71	77
Kuwait	80	80	74	82	76	76	76	78
Malaysia	74	71	67	74	71	73	68	71
Nepal	77	70	71	74	64	76	71	72
Oman	88	84	69	88	94	69	67	80
Pakistan	70	76	73	75	72	74	64	72

Country	Attitudes	Behavior	Cognition	Communication	Compliance	Norms	Responsibility	Security Culture Score
Philippines	73	69	69	74	72	74	65	71
Qatar	72	76	68	74	69	74	66	71
Saudi Arabia	75	75	72	77	70	76	67	73
Singapore	75	71	69	74	71	74	68	72
Sri Lanka	77	57	73	75	60	66	65	68
Taiwan	75	75	75	81	75	75	75	76
Thailand	75	72	70	73	71	67	47	68
Turkey	77	76	72	71	71	73	74	73
United Arab Emirates	72	69	68	75	69	72	66	70
Austria	78	81	69	75	69	75	73	74
Belgium	73	75	65	72	67	71	69	70
Bulgaria	79	84	81	80	83	85	79	82
Croatia	75	82	75	81	76	80	72	77
Denmark	74	78	69	72	72	75	70	73
Estonia	81	81	81	73	72	75	74	77
Finland	75	76	68	73	70	73	70	72
France	75	76	67	73	70	75	70	72
Germany	76	79	69	74	72	72	71	73
Greece	77	83	79	80	78	80	74	79
Greenland	70	68	62	69	63	64	65	66
Hungary	76	83	70	74	76	76	74	75
Ireland	75	75	70	72	69	74	69	72
Italy	70	72	65	71	67	71	69	69
Jersey	73	73	69	70	66	71	66	70
Lithuania	78	83	75	81	79	80	78	79
Luxembourg	72	76	66	70	67	72	70	71
Malta	76	74	72	77	72	73	71	74
Monaco	80	83	78	76	73	81	74	78
Netherlands	73	73	65	70	65	71	67	69
Norway	74	76	66	73	72	74	70	72
Poland	75	80	68	70	74	74	74	73
Portugal	77	81	68	71	71	77	71	74
Romania	75	78	76	81	72	80	77	77
Slovakia	79	84	74	73	77	77	75	77
Slovenia	73	72	66	72	67	71	66	70
Spain	76	79	70	76	74	76	71	75

Country	Attitudes	Behavior	Cognition	Communication	Compliance	Norms	Responsibility	Security Culture Score
Sweden	75	77	64	70	71	73	68	71
Switzerland	72	74	65	72	71	71	67	70
Ukraine	85	60	80	82	63	84	80	76
United Kingdom	75	78	69	72	72	74	69	73
Antigua and Barbuda	74	76	67	74	75	70	73	73
Bahamas	70	73	64	72	73	70	64	69
Barbados	70	68	61	64	57	64	70	65
Belize	72	71	67	72	67	70	69	70
Bermuda	70	76	70	72	74	72	68	72
Canada	75	74	70	74	72	73	69	72
Cayman Islands	81	75	75	78	77	72	75	76
Costa Rica	83	88	66	80	84	80	77	80
Dominica	70	67	67	63	48	70	72	65
Dominican Republic	80	86	65	79	81	81	70	77
Grenada	73	72	67	77	64	73	80	72
Honduras	80	80	63	77	77	74	70	74
Jamaica	71	71	70	72	69	70	69	70
Mexico	75	78	63	73	72	73	67	71
Nicaragua	78	81	64	75	75	76	70	74
Panama	78	87	64	77	80	81	71	77
Puerto Rico	78	80	64	73	74	76	68	73
Turks and Caicos Islands	72	71	67	73	75	71	69	71
United States	75	75	70	75	74	73	69	73
Australia	74	73	68	73	72	72	69	71
New Zealand	73	74	68	75	72	70	69	72
Papua New Guinea	71	75	60	67	65	73	71	69
Samoa	62	44	50	56	44	69	75	57
Brazil	73	76	68	70	68	77	67	71
Chile	75	75	63	77	76	72	71	73
Colombia	77	76	63	75	70	71	74	72
Curaçao	73	78	81	71	54	77	69	72
Ecuador	78	86	62	72	77	79	68	74
Paraguay	75	68	59	69	65	68	66	67
Peru	77	81	63	74	79	79	68	74
Trinidad and Tobago	74	74	69	70	74	70	70	71

States in the U.S. Data

State	Attitudes	Behavior	Cognition	Communication	Compliance	Norms	Responsibility	Security Culture Score
Alabama	74	75	71	76	75	73	69	73
Alaska	72	65	67	76	69	68	67	69
Arizona	72	75	66	70	70	71	66	70
Arkansas	73	72	69	77	74	72	68	72
California	75	76	71	76	75	74	69	74
Colorado	76	76	72	77	75	74	70	74
Connecticut	74	76	71	74	76	73	69	73
Delaware	77	79	72	75	77	76	71	75
District of Columbia	71	68	66	75	69	69	67	69
Florida	76	76	72	77	77	75	70	75
Georgia	74	74	70	75	75	72	69	73
Hawaii	72	68	69	75	70	69	67	70
Idaho	68	66	66	72	70	68	64	68
Illinois	74	75	68	73	72	73	69	72
Indiana	75	75	70	74	74	73	69	73
Iowa	74	74	69	75	74	72	69	73
Kansas	76	75	71	77	76	73	68	74
Kentucky	74	75	71	77	74	73	70	73
Louisiana	73	73	68	71	72	71	64	70
Maine	77	75	73	79	78	73	72	75
Maryland	79	78	74	78	79	77	72	77
Massachusetts	77	77	71	76	75	75	71	75
Michigan	75	74	71	75	73	73	70	73
Minnesota	75	75	70	76	75	73	71	74

State	Attitudes	Behavior	Cognition	Communication	Compliance	Norms	Responsibility	Security Culture Score
Mississippi	72	69	69	76	73	71	66	71
Missouri	74	74	70	75	73	72	69	72
Montana	75	77	72	74	74	75	69	74
Nebraska	75	77	69	78	76	74	68	74
Nevada	74	76	70	74	75	73	67	73
New Hampshire	75	76	70	78	76	74	71	74
New Jersey	75	76	70	74	74	74	69	73
New Mexico	79	79	74	80	74	75	73	76
New York	74	74	71	77	74	74	69	73
North Carolina	73	72	69	74	72	72	68	71
North Dakota	80	82	74	75	79	77	72	77
Ohio	75	75	70	75	74	73	70	73
Oklahoma	78	78	72	77	78	75	71	76
Oregon	76	76	71	76	75	74	69	74
Pennsylvania	74	74	69	74	72	72	68	72
Rhode Island	75	76	72	80	77	75	71	75
South Carolina	75	74	71	77	76	73	70	74
South Dakota	77	79	72	74	77	73	71	75
Tennessee	73	73	69	73	73	71	68	71
Texas	75	75	71	75	75	74	69	73
Utah	73	75	70	76	73	73	70	73
Vermont	75	75	71	77	73	73	72	74
Virginia	75	75	71	75	75	73	69	73
Washington	78	80	73	76	76	77	71	76
West Virginia	75	75	71	73	75	72	68	73
Wisconsin	74	75	68	72	73	72	69	72
Wyoming	73	73	71	77	74	72	68	72

Authors

Anna Collard

is Senior Vice President of Content Strategy & Evangelist for KnowBe4 Africa where she drives security awareness across the African continent. Collard founded security content publisher Popcorn Training, which was acquired by KnowBe4 in 2018. She has won many tech and cybersecurity industry awards throughout Africa and globally and is a member of the World Economic Forum's Global Future Council on the Future of Metaverse for the 2023-2024 term.

Megan Colbert

is the Project Coordinator to the Chief Evangelist and Strategy Officer. She holds a Master's Degree in Strategic Innovation and Change Management. Throughout the onset of her career, she has garnered experience across multiple sectors, notably in cybersecurity, hospitality and education. Colbert is a collaborating author on this report.

Joanna Huisman

is Senior Vice President of Strategic Insights and Research at KnowBe4. She is a cybersecurity, training and communications expert 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 is the project manager and lead author of this report.

Dr. Martin J. Kraemer

is a Security Awareness Advocate at KnowBe4. He has over 10 years of research and industry experience in cybersecurity with a focus on human-centered computing. Martin held roles in innovation, research and technology consulting. He has worked with both public and private organizations on information security and data protection.

Authors (Continued)

Javvad Malik

is the Lead Security Awareness Advocate at KnowBe4 and is based in London. Malik is an IT security professional with over 20 years of experience as an IT security administrator, consultant, industry analyst and security advocate. He has won multiple industry awards and is currently a Guinness World Records holder for the most views of a cybersecurity lesson on YouTube in 24 hours.

Erich Kron

is a Security Awareness Advocate at KnowBe4. He is a veteran information security professional with over 25 years of experience in the medical, aerospace manufacturing and defense fields. Kron is also an author, prolific speaker and regular contributor to cybersecurity industry publications. He is the former security manager for the U.S. Army's 2nd Regional Cyber Center-Western Hemisphere and holds the CISSP, CISSP-ISSAP, SACP and many other certifications.

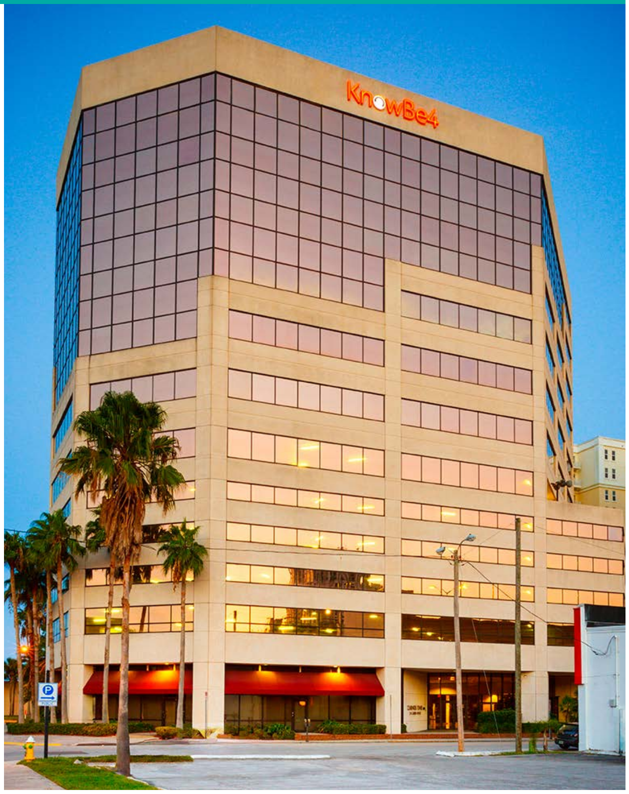
Rosa L. Smothers

has over 20 years of experience in cybersecurity. Most recently she was senior vice president of cyber operations at KnowBe4, where she provided cybersecurity advisory services to civilian and military agencies within the U.S. federal government. Smothers is a collaborating author on this report.

Miha Matjašič

is a multifaceted researcher and academic associated with two faculties at the University of Ljubljana, Slovenia, where he specializes in survey methodology and statistical analyses within this domain. His expertise extends to applied survey methods and a deep understanding of statistical and data mining concepts, including multivariate analysis, significance testing, regression, decision trees, clustering, forecasting, sampling, simulation and advanced modeling.

About Us



Join the Discussion

Thank you for your interest in this report. We're glad you took the time to dive into its contents. If you find the insights valuable and wish to engage in further conversations, we encourage you to share the report and express your thoughts on social media or other online platforms of your choosing.

When referring to the report, kindly use its full title: "Security Culture Report 2024 by KnowBe4 Research." If you're considering sharing the report with others, we kindly request that you share the link instead of the PDF file itself to ensure that the most current version is always being used.

For any press-related questions or detailed discussions, please get in touch with our Public Relations team at PR@KnowBe4.com.

KnowBe4
Research

As KnowBe4's specialized research division, KnowBe4 Research is devoted to producing exceptional inquiries into security awareness, human behaviors and organizational culture. This is achieved through an integrated analysis of comprehensive datasets such as the Security Culture Survey alongside empirical behavior data, knowledge assessments and extensive training materials that reach millions of employees. KnowBe4 Research undertakes thorough examinations to uncover the optimal strategies for organizations to mitigate risks.

Harnessing the power of billions of data points and empowering rigorous scientific techniques, KnowBe4 Research aims to enhance and elevate the effectiveness of security awareness, behavior and culture across the board.

About KnowBe4

KnowBe4 empowers your workforce to make smarter security decisions every day. Tens of thousands of organizations worldwide trust the KnowBe4 platform to strengthen their security culture and reduce human risk. KnowBe4 builds a human layer of defense so organizations can fortify user behavior with new-school security awareness and compliance training.

KnowBe4, Inc.
33 N Garden Ave, Suite 1200
Clearwater, FL 33755

www.KnowBe4.com
Sales@KnowBe4.com

Tel: 855-KNOWBE4 (566-9234)