KnowBe4 Research

SECURITY CULTURE REPORT FOR **AFRICA** 2024

KnowBe4's 2024 Security Culture Report dives deep into how security measures affect organizations and the way employees act and feel at work. It stands out as the most in-depth and comprehensive analysis of security culture available, and presents survey findings from thousands of organizations across the globe and a rich five-year comparative perspective.

The report presents an intricate and exhaustive examination of six global regions, assessing each one's security culture readiness, encompassing North America, South America, Europe, Africa, Asia and Oceania.

This guide provides an overview of the key findings for Africa.

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**

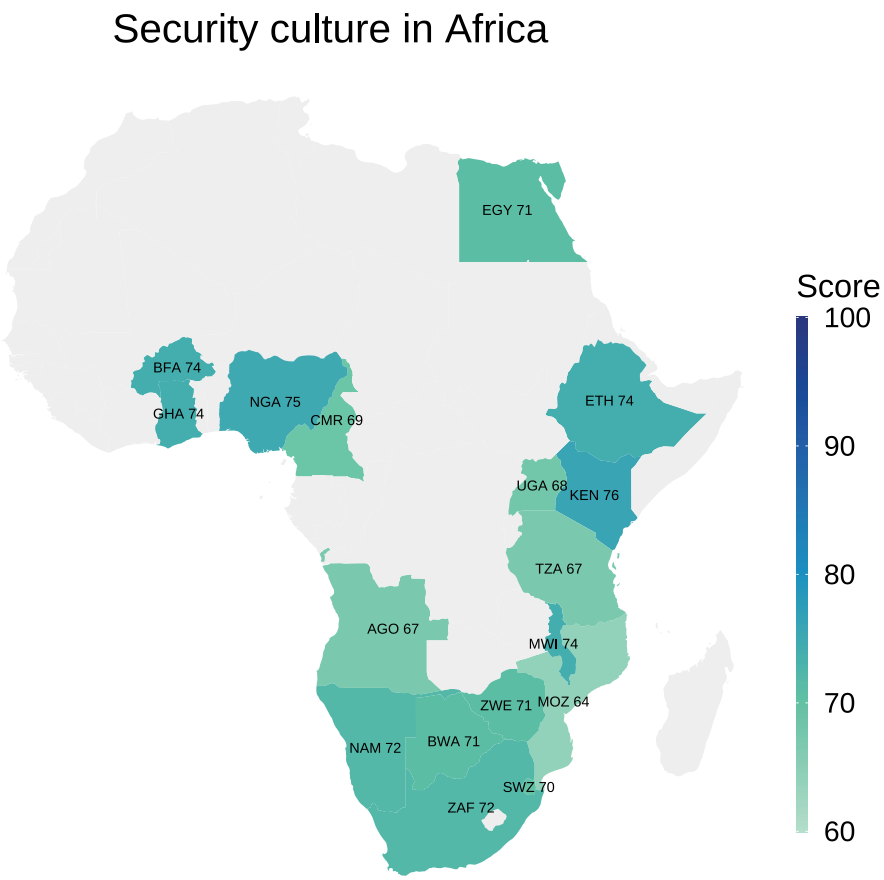
Note: None of the industry sectors have demonstrated Excellent or Good security culture this year.

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.

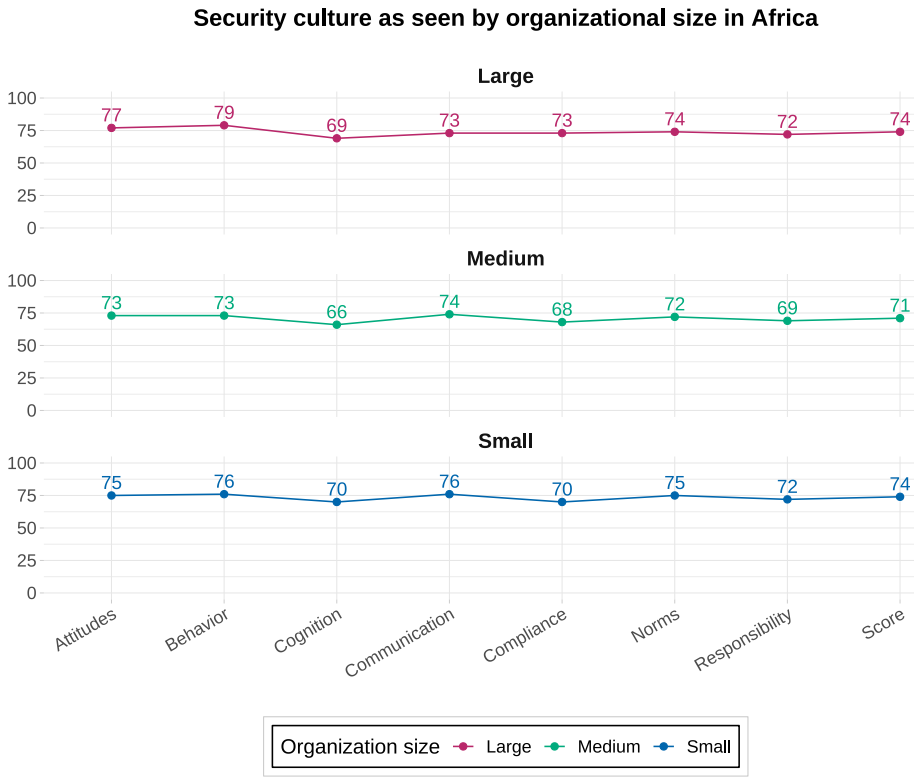
The best-performing African countries in this report are Kenya, Nigeria and Ghana, all which have more mature cybersecurity strategies driven by their local governments. In fact, Ghana's cybersecurity success has boosted it from 89th place to 43rd on the 2020 International Telecommunications Union's 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.



Key Takeaways

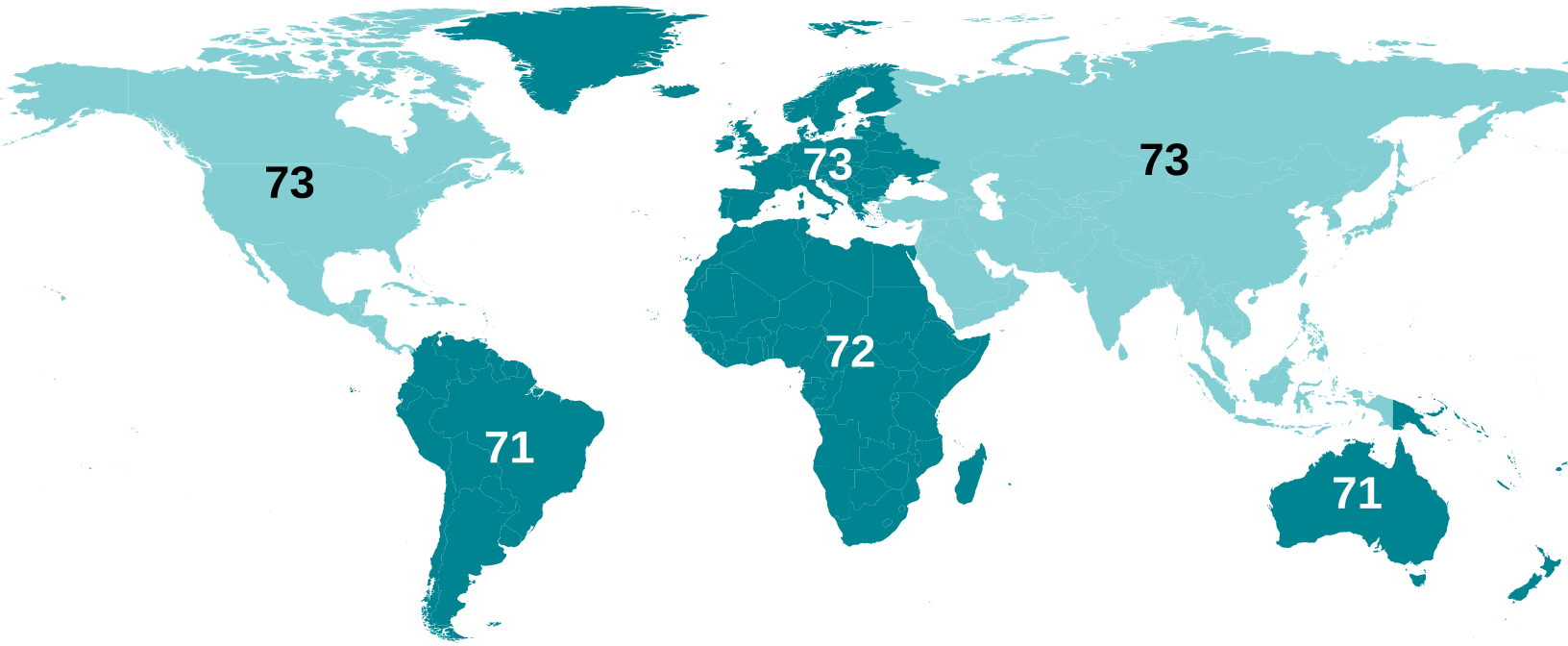
The South African Council for Scientific and Industrial Research (CSIR) expects an increase in cyber attacks on government departments and critical infrastructure, impacting not just private sector organizations but also societies and national economies.

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.

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.

Global Overview

By Javvad Malik, Lead Security Awareness Advocate

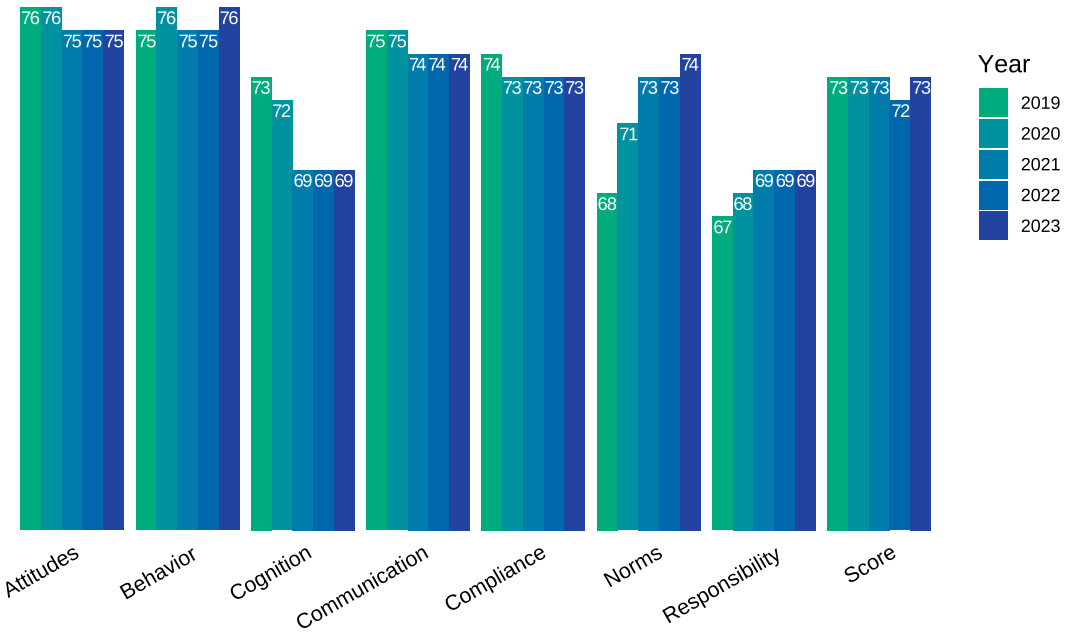


Cultural Adoption

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.

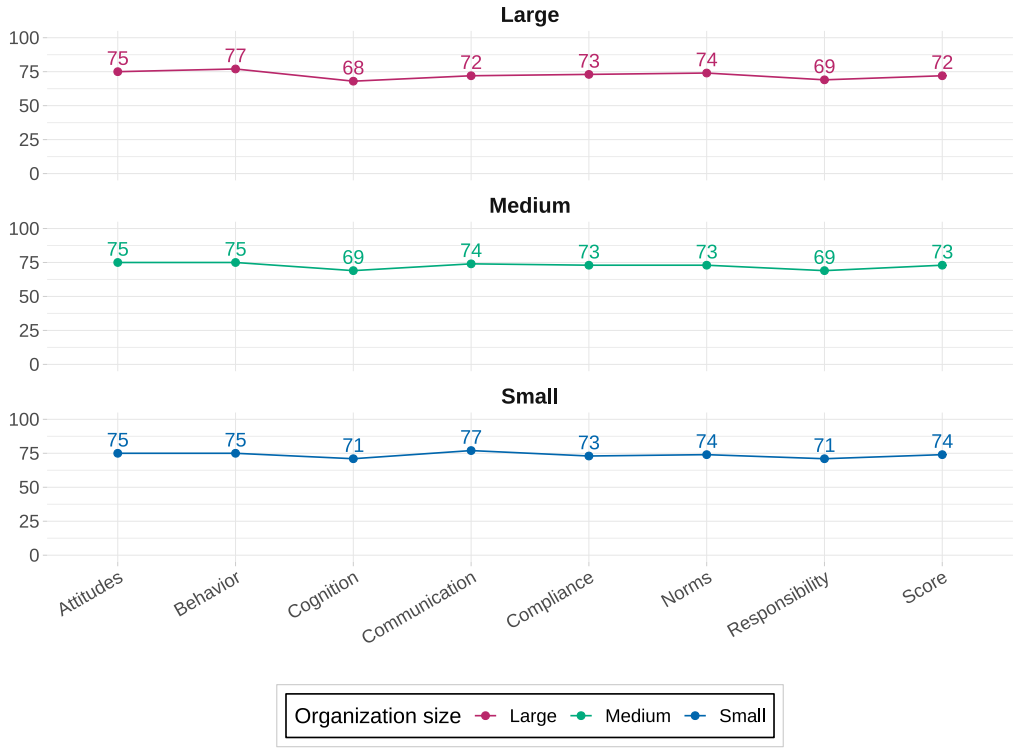
Organizations around the world vary greatly in how deliberate they are in building a strong security culture that aligns with their risk tolerance and overall culture. While many governments and organizations have attempted to implement some form of cybersecurity strategy, their efforts have met varying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

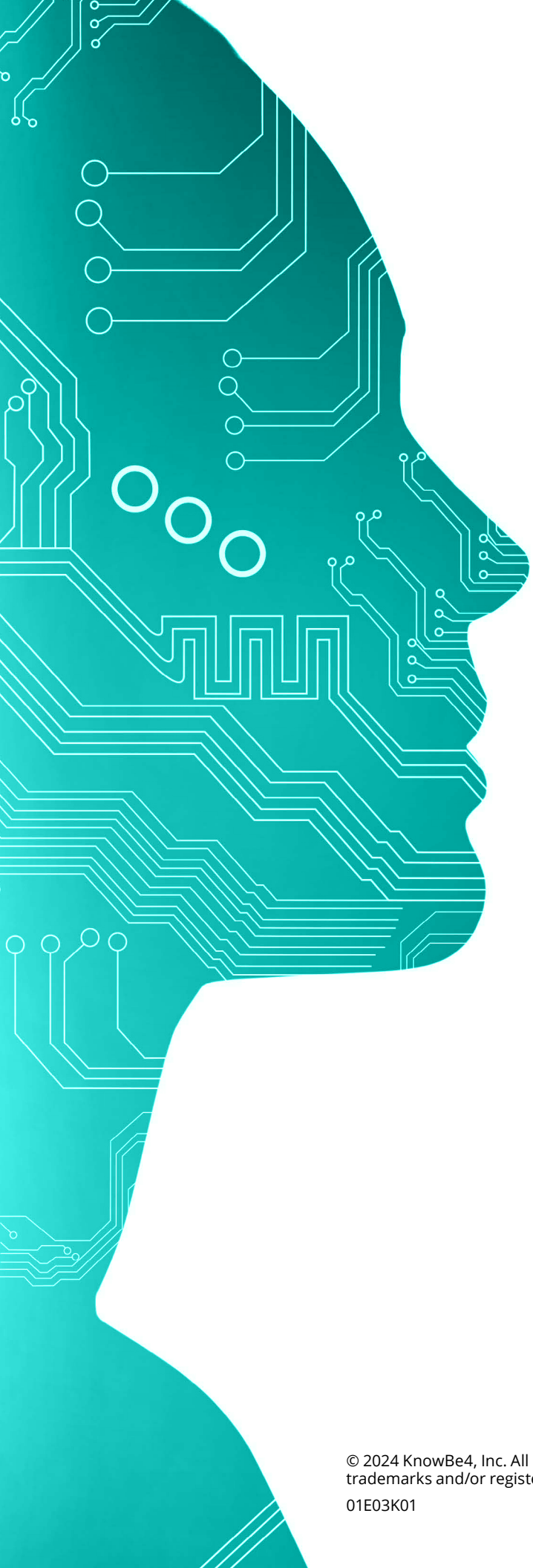
As the COVID-induced panic buying of toilet rolls was starting to wane, global events introduced a new set of complex risks. In 2022, Russia invaded Ukraine, while the following year brought escalating conflict in the Middle East. These are significant because we've seen how cybersecurity has played 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."

Read The Full Report

01E03K01