KnowBe4 Research

SECURITY CULTURE REPORT FOR **EUROPE** 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 Europe.

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.

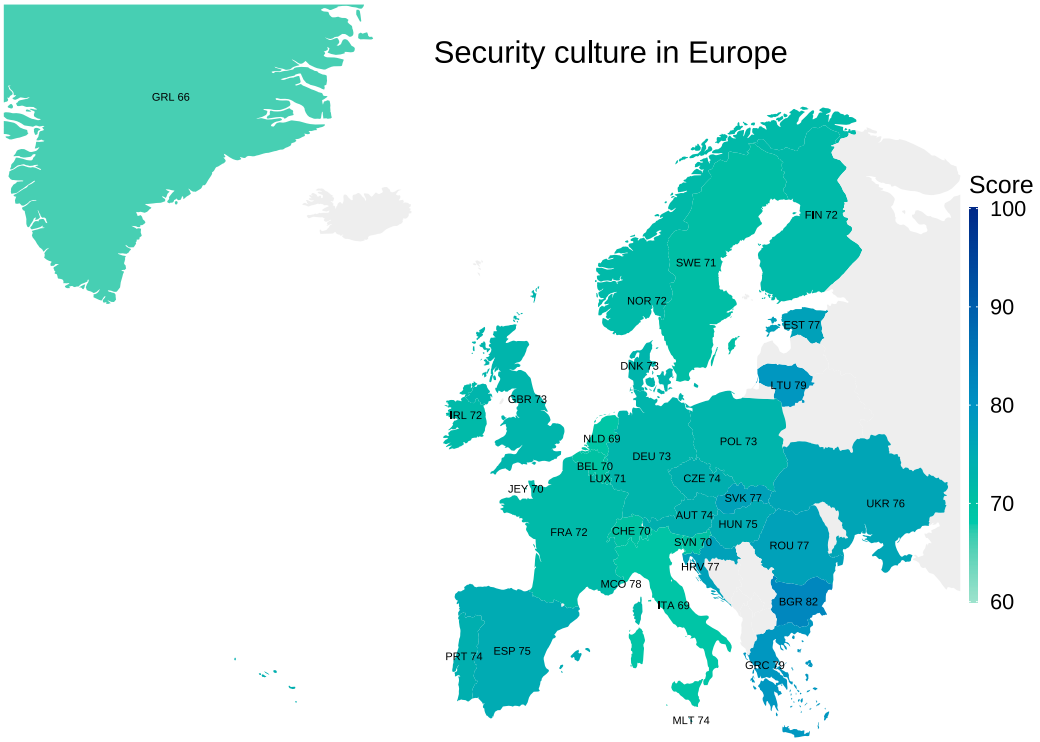
Europe

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

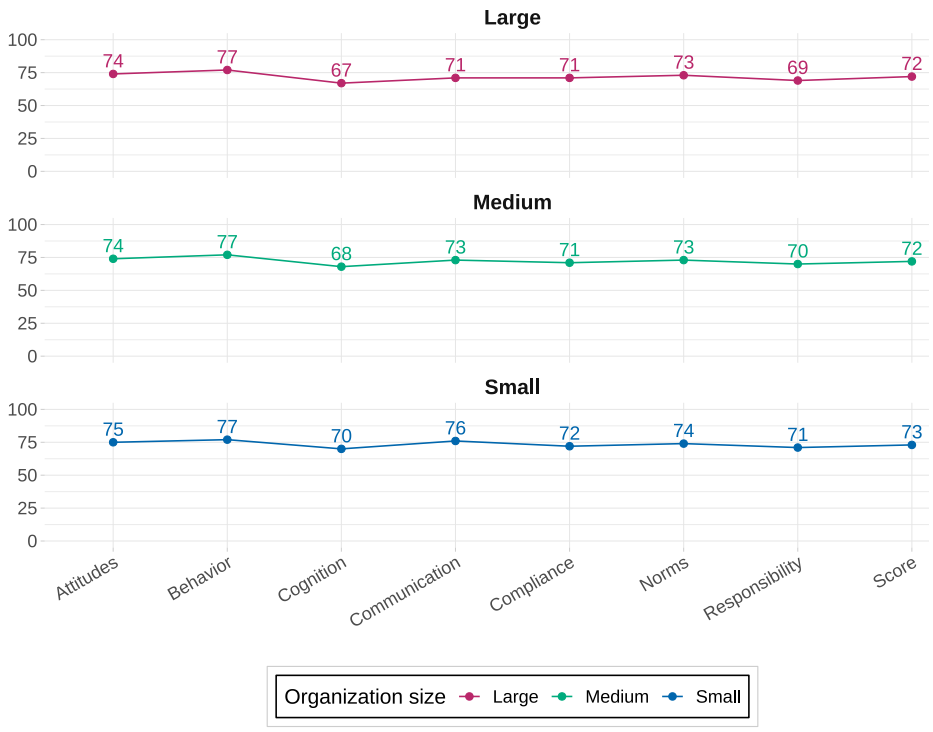
The European Union Agency for Cybersecurity (ENISA) reports an increase in quality and quantity of cyber attacks and their consequences, a surge in ransomware attacks for 2023, and influences from the Russia/Ukraine conflict. The top three threats were ransomware, malware and social engineering. 2023 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.

Security culture as seen by organizational size in Europe



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

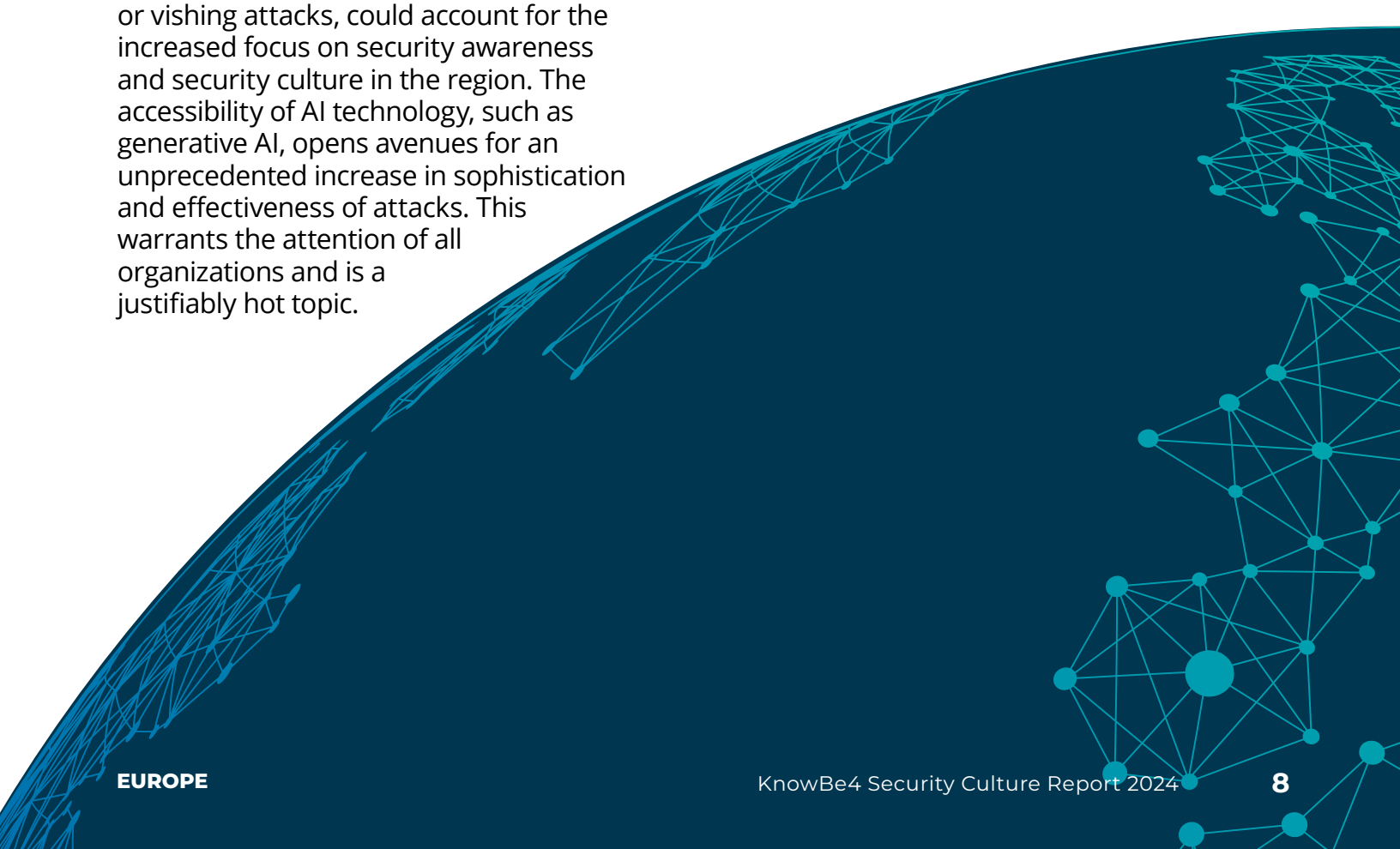
We can report similar influences of AI in Europe as in the rest of the world. The cybersecurity threat landscape evolves with phishing attacks gaining in quantity and quality. Misinformation and disinformation will also be fueled by generative AI, which ENISA already considers a cybersecurity threat.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

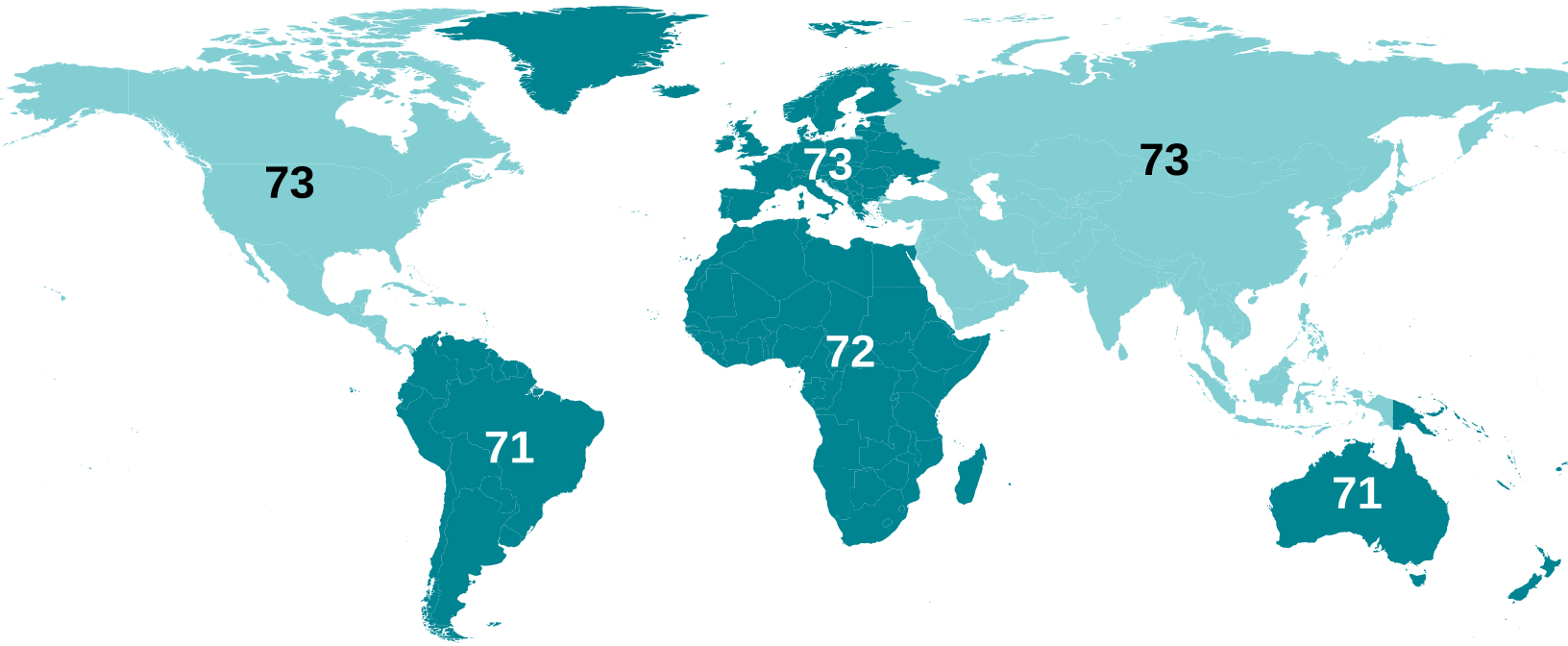
Generative AI-driven misinformation is becoming a growing concern, while significant breaches like MOVEit and Clop gang's extortion tactics are influencing cybersecurity reporting regulations, credit security measures and insurance industry responses to ransomware and data leaks.

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.

Global Overview

By Javvad Malik, Lead Security Awareness Advocate

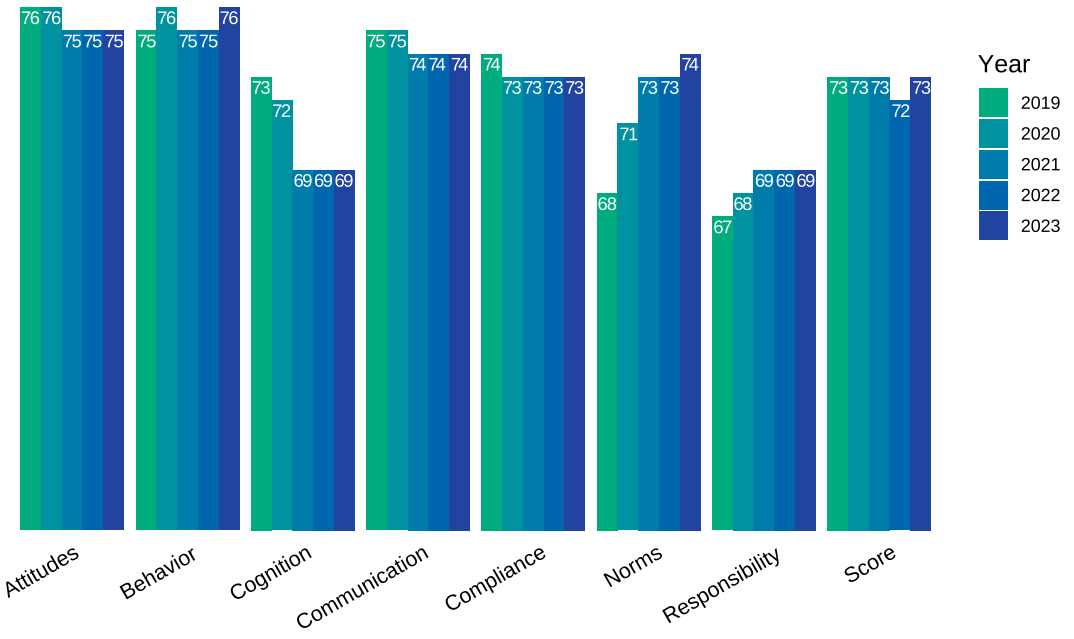


Cultural Adoption

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.

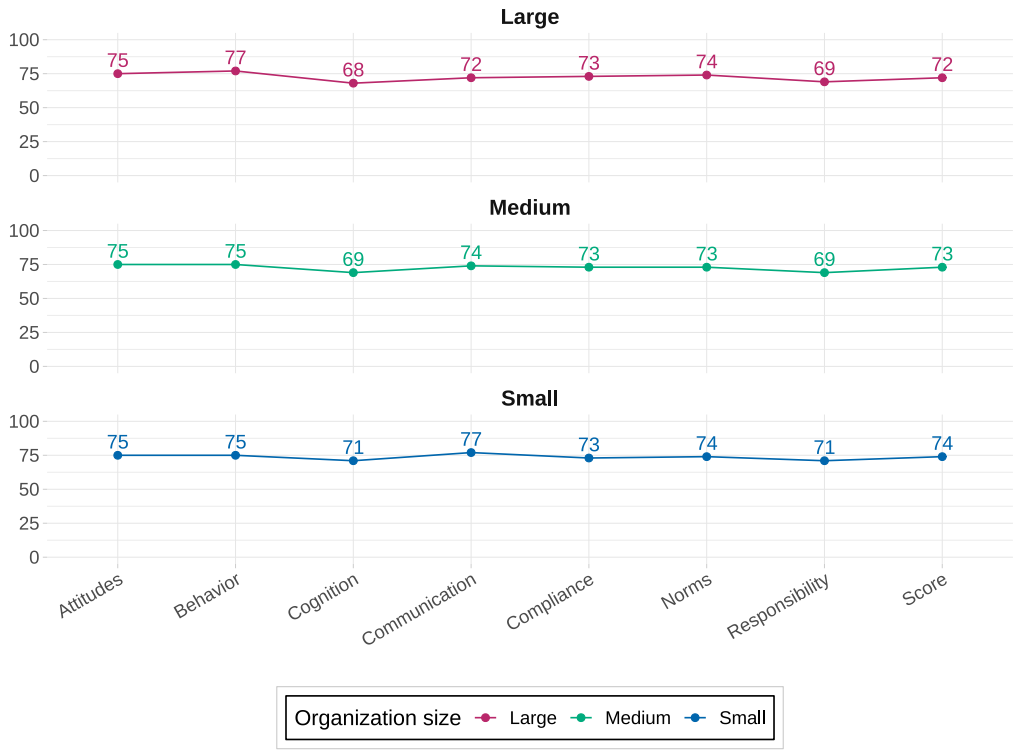
Organizations around the world vary greatly in how deliberate they are in building a strong security culture that aligns with their risk tolerance and overall culture. While many governments and organizations have attempted to implement some form of cybersecurity strategy, their efforts have met varying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

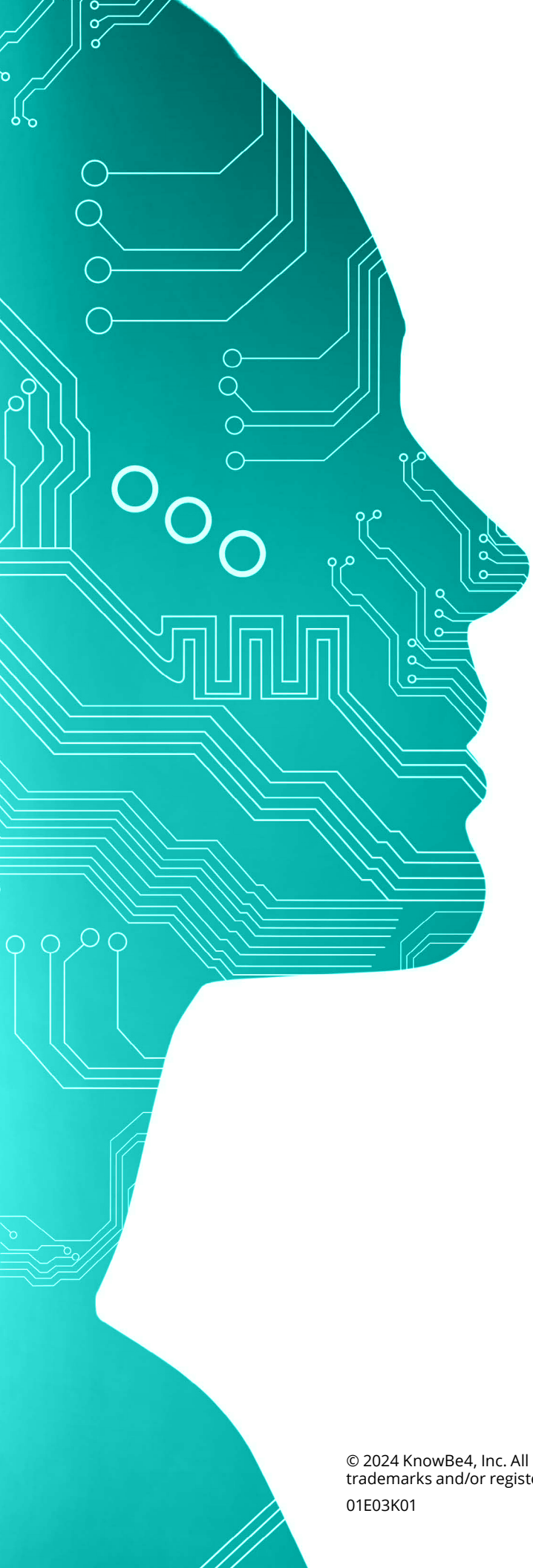
As the COVID-induced panic buying of toilet rolls was starting to wane, global events introduced a new set of complex risks. In 2022, Russia invaded Ukraine, while the following year brought escalating conflict in the Middle East. These are significant because we've seen how cybersecurity has played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