



EXPERTS WITH IMPACT™

CyberCulture Scan

Building a Robust, Ready and Resilient Cybersecurity Culture

**PUTTING PEOPLE AT THE CENTER
OF CYBERSECURITY RESILIENCE**



Organizations have never been more vulnerable to the human element of cyber and data security: In fact, human decisions and behaviors trigger more than two out of three incidents.¹ An organization's cybersecurity culture can either contribute to its protection or introduce risk.

Marrying Cybersecurity Communications With Organizational Culture

When it comes to cybersecurity, people are considered an organization's greatest vulnerability – but they also have the potential to become the greatest asset. Increasing employees' understanding that cybersecurity is a shared responsibility empowers them to mitigate data security risks for the broader organization, making a strong cybersecurity culture an organization's strongest line of defense.

Leveraging our extensive experience in business transformation and change management together with our deep expertise in Cybersecurity and Data Privacy Communications, we believe businesses can greatly benefit from proactively conducting a cybersecurity culture scan, which at FTI Consulting, we refer to as the "CyberCulture Scan", to determine gaps and opportunities to enhance cybersecurity resilience.

FTI Consulting's [CISO Redefined: Navigating C-Suite Perceptions & Expectations](#) 2024 study demonstrates that executive leaders recognize the need for a strong cybersecurity culture as crucial to prevent threats: C-suite executives cite "approaches to building a proactive and adaptive cybersecurity culture" as one of their top five CISO communications training priorities.²

Cybersecurity culture refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms, and values people have about cyber and data security in an organization's day-to-day operations.

However, most organizations do not yet assess their cybersecurity culture systematically or holistically; technology solutions and phishing tests alone do not comprise a healthy cybersecurity culture check. They don't reveal the behavioral decisions employees make about cybersecurity and data privacy. Without assessing the intangible drivers of the current cybersecurity culture, organizations miss the opportunity to integrate cybersecurity considerations into employees' habits and day-to-day actions.

Building a strong culture of cybersecurity: What you measure you can manage

CyberCulture Scan: a 3-phased approach

To help organizations fill the cybersecurity culture void, our CyberCulture Scan offers a proprietary assessment tool to implement a three-phased approach to incorporate employees into the equation when building a strong cybersecurity culture:



1. Assess the current cybersecurity culture

Understanding what motivates and influences behavior unlocks valuable insights that organizations can leverage in training programs, employee communication and culture change initiatives. FTI Consulting's proprietary assessment tool delivers detailed insights into an organization's cybersecurity culture strengths and weaknesses.



2. Embed cybersecurity-conscious behaviors

Adopt a management approach that helps integrate a cybersecurity mindset into the fabric of an organization's operations. This involves defining clear and measurable outcomes that reflect the desired cybersecurity posture and ensure all levels of the organization understand and embrace the processes to achieve these outcomes. Setting clear objectives; aligning structures, governance and ways of working with the desired culture; and integrating cybersecurity practices into talent management create a coherent culture and aligned framework that ultimately minimizes risk.



3. Enable the desired cybersecurity culture

Actively fostering and enabling the cybersecurity culture through targeted initiatives aimed at transforming employee mindsets and behaviors. This phase ensures the aspirational aspects of the cybersecurity culture translate into practical, everyday actions. We deploy change management, training, communications, and continuous assessment tools to enable employee understanding and willingness to adopt new mindsets and behaviors.

CyberCulture Scan methodology

We employ a comprehensive **six-step methodology** to provide organizations with a rich understanding of employees' behavioral decisions about cybersecurity and data privacy and clear direction about where to focus efforts to strengthen the cybersecurity culture.



1

Backgrounding

Desk-level research, materials request and review, and a client workshop to ensure we understand the business, the organization, its primary security (cybersecurity, data privacy, etc.) risk areas and history.

2

1:1 Leader Interviews

Confidential discussions to understand leaders' perceptions of how security advances business strategy, its connection to current culture and priorities for improvement.

3

Cybersecurity Culture Diagnostic

Our CyberCulture Scan assessment is designed to uncover the beliefs, mindsets and behaviors of employees toward cybersecurity to understand strengths, risks and opportunities. The assessment delivers a scorecard for benchmarking and performance tracking.

6

Strategic and Tactical Planning

The leadership activities, communications, enablement, engagement and measurement programs that will shift the culture toward the desired state.

5

Key Findings and Next Steps

A strategic approach to embedding security mindsets, behaviors and leadership into organizational culture customized based on the Cybersecurity Culture Diagnostics and focus group findings.

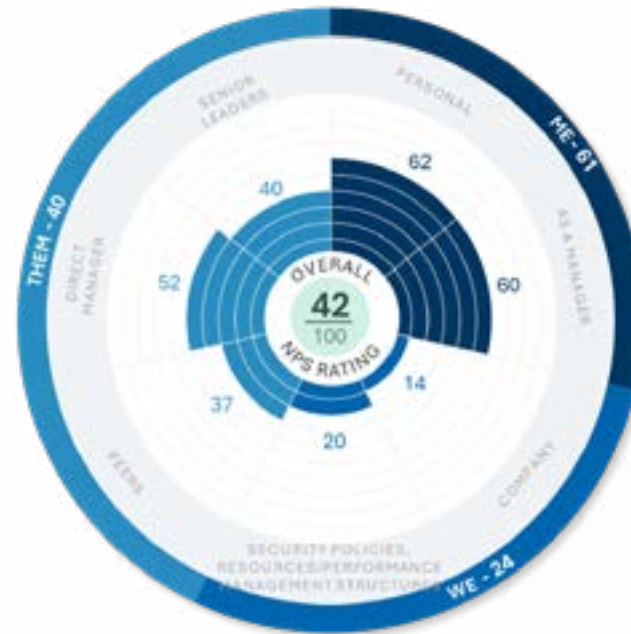
4

Validation Workshop

Validation of and deeper investigation into key challenges and barriers revealed in the Cybersecurity Culture Diagnostics employee survey.

Assessment output

Our proprietary assessment tool produces a **detailed overall cybersecurity culture scorecard** that serves as a benchmark for measuring progress. This scorecard provides an aggregate culture rating and breaks down specific scores across various dimensions of cybersecurity culture. This detailed analysis identifies strengths and pinpoints areas for improvement, facilitating targeted strategy development and deployment for maximum impact.



FOR MORE INFORMATION, CONTACT OUR EXPERTS:

JAMIE SINGER

Senior Managing Director, Cybersecurity & Data Privacy Communications, U.S.
Jamie.Singer@fticonsulting.com

FLORENCE HUGENHOLTZ

Managing Director, Cybersecurity & Data Privacy Communications, U.S.
Florence.Hughenoltz@fticonsulting.com

MEGAN BRUNET

Senior Director, Strategic Communications, People & Transformation, U.S.
Megan.Brunet@fticonsulting.com

MADELYN HAWKINS

Senior Director, Cybersecurity & Data Privacy Communications, U.S.
Madelyn.Hawkins@fticonsulting.com

CHARLOTTE LEEMAN

Senior Director, Strategic Communications, Corporate Reputation, Belgium
Charlotte.Leeman@fticonsulting.com

SASCHA ULLRICH

Senior Director, Strategic Communications, People & Transformation, Germany
Sascha.Ullrich@fticonsulting.com

¹ "2025 Data Breach Investigations Report," Verizon business (last accessed April 7, 2025), <https://www.verizon.com/business/en-au/resources/reports/dbir/#snapshots>.

² "CISO Redefined: Navigating C-Suite Perceptions and Expectations," FTI Consulting (March 2024), <https://fticonsulting.com/ciso-redefined-navigating-c-suite-perceptions-and-expectations/>.

FTI Consulting is the leading global expert firm for organizations facing crisis and transformation, with more than 8,300 employees in 34 countries and territories. FTI Consulting is dedicated to helping organizations manage change, mitigate risk and resolve disputes: financial, legal, operational, political and regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities.
 © 2025 FTI Consulting, Inc. All rights reserved. fticonsulting.com