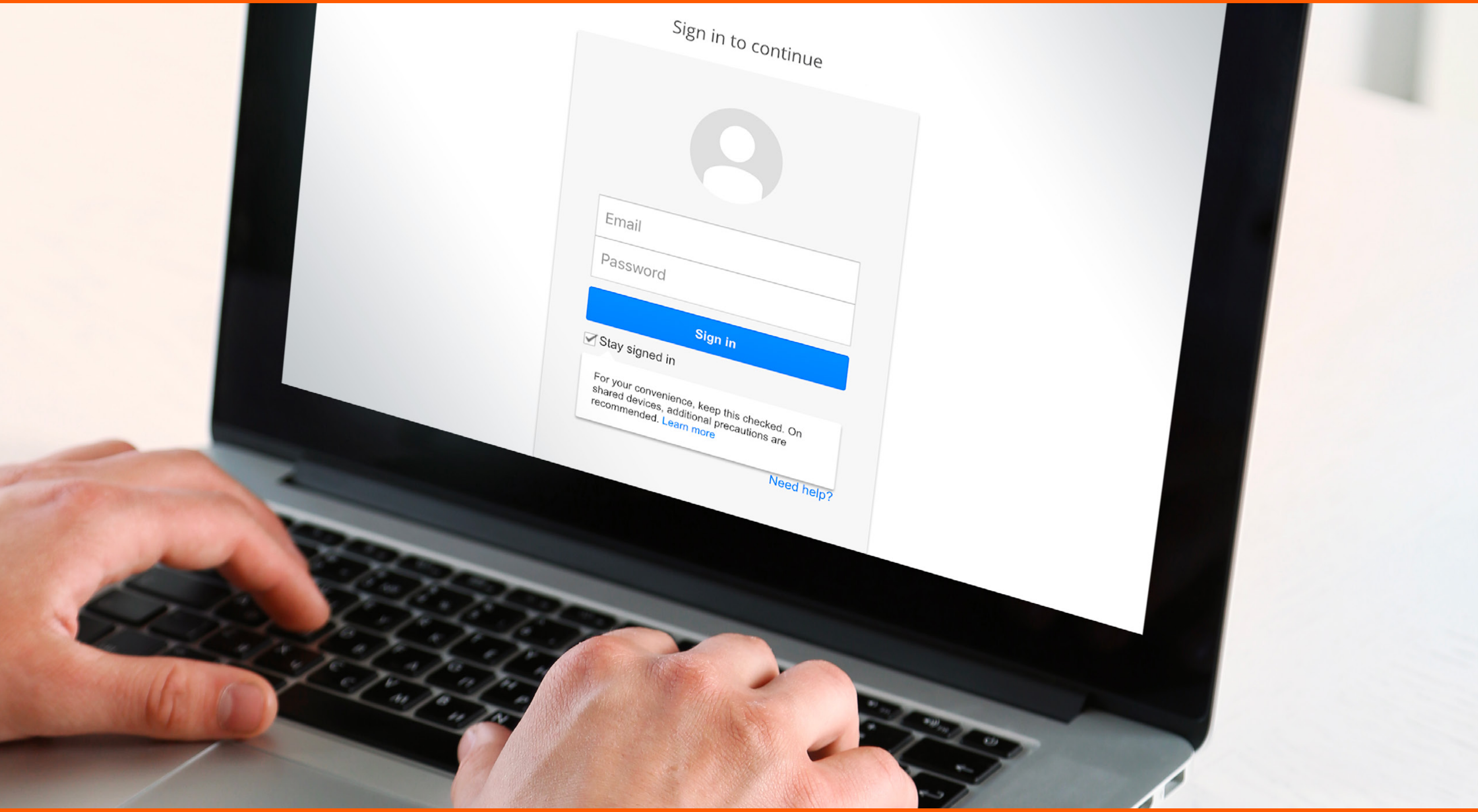
cortrucent
TECHNOLOGIES

KnowBe4
Human error. Conquered.


Sign in to continue
Email
Password
Sign in
Stay signed in
For your convenience, keep this checked. On shared devices, additional precautions are recommended. Learn more
Need help?

WHITEPAPER

How Security Culture Invokes Secure Behavior

INTRODUCTION

For a long time, organizations have looked for ways to improve their security posture and reduce risk. They have turned to technology as a primary means to do this and have found that technology is only a single ingredient in a more complex recipe. Social engineering, or phishing to be more precise, is the go-to means of entry by hackers because it works. Based on data from the 2020 Verizon Data Breach Investigations Report, we believe attacks on the human layer are now responsible for a majority of events leading to breaches.

Humans, often to be considered a major weakness in an organization's battle against cybercrime, have now become one of the greatest assets in the fight to help organizations be better protected. Equally important to this realization, is how you prepare your workforce to withstand the attacks that are lurking behind their emails daily.

IT leaders know that a well-designed security strategy consists of a combination of people, process, and technology. But with technology and processes often being pushed towards the forefront, the human element in cybersecurity is often overlooked. One of the reasons for this is the apparent difficulty for organizations to provide interesting and engaging awareness training, and consequently creating secure behavior.

A primary means to cultivate and maintain secure behavior in organizations is through intentional focus on the organization's security culture. Security culture, although part of the overall company culture, leans towards a key difference. Whereas company culture is a set of shared values, goals and practices that characterize an organization, security culture involves the shared ideas, customs and social behaviors that influence security. Furthermore, this is when employees internalize what their individual roles and responsibilities are to better protect and defend, not only their professional environment, but their personal one, too. By focusing on improving security culture, an organization will raise their security readiness; and their people will begin to instinctively act as an effective protective layer.

It has always been suspected that security culture and secure behavior were closely linked, although proof was hard to produce. Until now. Through KnowBe4's groundbreaking research, not only have we been able to validate that link, but we also provide data that provides conclusive evidence related to the importance of focusing on the human element. By examining the behavior and security culture of 97,661 employees across 1,115 organizations, KnowBe4 has observed that the link exists between the level of security culture in an organization and the measure of secure behavior of its employees.

Security culture is affected by a set of seven core Dimensions:

- **Attitude**—the feelings and beliefs that employees have towards security protocols and issues.
- **Behavior**—the actions and activities of employees that have direct or indirect impact on the security of the organization.
- **Cognition**—the employees understanding, knowledge and awareness of security issues and activities.
- **Communication**—the quality of communication channels to discuss security-related events, promote 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.
- **Responsibility**—how employees perceive their role as a critical factor in sustaining or endangering the security of the organization.

The dataset used to identify these patterns combines the measured behaviors of employees, as measured using the KnowBe4 Kevin Mitnick Security Awareness Training (KMSAT) phishing assessment platform, and the measured security culture of the organizations of the same employees, as collected through our scientific Security Culture Survey.

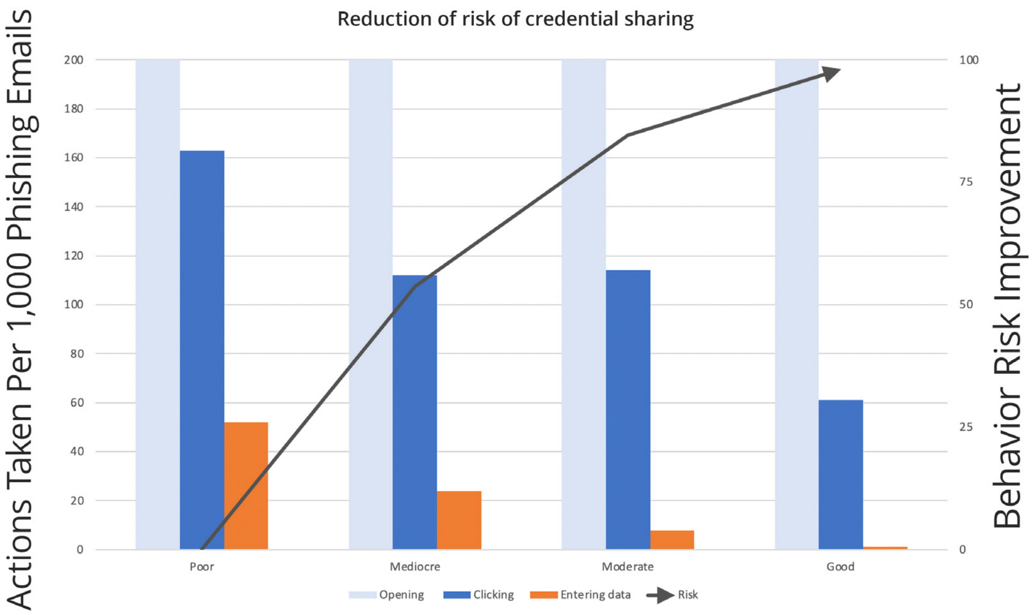
THE EFFECTS OF SECURITY CULTURE ON RISK

Our findings conclude that organizations that invest in building and maintaining a security culture will drive significantly higher secure behaviors among their employees. In fact, there is a 52x difference between the behaviors of credential sharing in the worst class (Poor) and the best class (Good). This means the more focus given to security culture, the greater the likelihood that employees will follow secure practices and adopt more secure behaviors.

The classes are categorized according to the security culture score of organizations included in the dataset on which the research is based. The results were staggering:

	Mediocre	Moderate	Good
Poor	2x	6x	52x
Mediocre	—	3x	24x
Moderate	—	—	8x

Table: *Change in mean risky behavior (credential sharing) by improved Security Culture Score*



Graph: *Reduction of risk of credential sharing. This graph shows the number of actions (out of 1,000) taken by employees. The columns represent the different actions (Opening, Clicking, Entering Data), and the column groups represent the security culture class. The black line shows how the risk is reduced by moving from one class to another.*

CONCLUSION

Improving one's security culture directly translates into more secure employee behaviors and to the overall reduction of organizational risk. While investment may have been difficult to obtain in the past, this research shows a strong return on such an investment and additional value.

Consider these steps your organization can take to build upon:

- ***Risk Assessments***—set-up periodic assessments, or better yet, continuous monitoring of your organizations risks. Make sure that your risk assessment includes the human factors as measured by security culture, knowledge and behavior of the organization and its employees.
- ***Use the 7 Dimensions***—actively work on building a strong security culture using the seven dimensions as a guideline for improvement.
- ***Train and measure through engagement and automation***—partner with KnowBe4 to design and automate the right awareness training program to fit your diverse audience, including engaging content, attack simulations and unique communication tools.
- ***Communicate often***—communicate often by partnering with other departments and connecting their messages to overall security initiatives.
- ***Use the Champion Model***—consider mobilizing a champion program across your organization in order to have advocates in every department, region and country who can further translate and embed the security message within your organization.
- ***Engage with your peers***—the security landscape is always changing and it is difficult to keep track of it all. Leverage your security community to learn from others, and to share your own knowledge and experience.

Additional Resources

Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain

About KnowBe4

KnowBe4 is the world's largest integrated security awareness training and simulated phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the ongoing problem of social engineering through a comprehensive new-school awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing, and vishing attacks and enterprise-strength reporting, to build a more resilient organization with security top of mind.

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make smarter security decisions.