THE CYBERSECURITY CULTURE CHALLENGE

Consider the following questions and findings from ISACA and CMMI Institute's new *2018 Cybersecurity Culture Study* to discover how your organization compares to others around the world.

1. **MINDING THE GAP.** Is there a significant gap between the current and desired state of your organization's cybersecurity culture? Getting employees on board with your cybersecurity program is a challenge for many organizations—but must be done to have the culture your organization needs.

2. **BEHAVIOR IS EVERYTHING.** Policies are pivotal, but employees don't always pay attention to them. How would you characterize the health of your cybersecurity culture as measured by its collective online behavior?

3. **ONE STEP AHEAD.** Beyond employee training, organizations that seek to transform their cybersecurity culture may also consider options such as improving management participation and the way they communicate behavioral policies. Which steps will your organization take to improve its culture now and within 12 months?

4. **TAKING PROPER MEASUREMENTS.** For organizational leaders, keeping a finger on the pulse of staff views about cybersecurity is rarely job #1. Has your organization measured or assessed employee views about its cybersecurity culture in the past year?

5. **A MATTER OF TRUST.** Investing in your organization can help build employee trust and narrow the gap between your current and desired culture. How confident are you in your organization's ability to manage or transform its cybersecurity culture?

6. **SAFETY IN NUMBERS.** There are many ways to spread better organizational habits when it comes to protecting your enterprise, including establishing clear and consistent policies. What are the next most important steps your organization can take to strengthen its cybersecurity culture? Rewards? Champions?

7. **GREAT EXPECTATIONS.** In many organizations, cybersecurity culture success is inhibited by factors such as a lack of executive buy-in, improper funding, a lack of tools or hands-on training. What prevents your organization's cybersecurity culture from meeting expectations?

8. **SIZE AND SUCCESS.** Is it easier for larger or smaller organizations to get all of their employees on the same page about defending the enterprise? In general, larger organizations have more resources, but they may also have more disparate business units and operate in multiple regions. See the ISACA/CMMI report to gauge how your organization's quest to obtain employee buy-in compares to others its own size, in its own region or key industries.

Looking to improve your organization's cybersecurity culture? Read *ISACA and CMMI Institute's 2018 Cybersecurity Culture Report: Narrowing the Culture Gap for Better Business Results* to learn how to build and manage a more effective cybersecurity culture.

ISACA® CMMI® Institute AN ISACA ENTERPRISE

www.isaca.org/cybersecurity-culture-study