The Proof: Surveying Your Organization

Business guru Peter Drucker once said, “If you can’t measure it, you can’t improve it.” If you’re going to the effort of improving cybersecurity at your organization with cybermindfulness education, you’re going to want to know if it’s working.

Measuring the effectiveness of your training program with a survey gives you a way to show end users and other stakeholders that it’s working, too. This guide will help you measure your organization’s movement towards cybermindfulness.

Measuring Awareness, Agency, and Action

The questions below will help demonstrate that the cybermindfulness training program has improved your organization’s:

- Desire to protect themselves and others in the organization from cyber threats
- Ability to identify social engineering ploys
- Knowledge of strategies for defending against such attacks

Sweeten the Pot

If you have a budget for your cybersecurity training efforts, survey time is a great time to have a drawing or offer people a small gift or promotional cybersecurity swag, like a webcam cover or encrypted USB drive, to incentivize participation. It’s an excellent way to make your organization feel extra warm and fuzzy about the IT team—and increase the chances people feel comfortable reaching out for help if they fall for a social engineering ploy.

Sample Surveys

Using the Sample Survey

You can distribute hard copies of the sample survey, found on page 3, within your organization or enter the questions into a tool like Survey Monkey or Google Forms and distribute it electronically. Whichever works best for you.

Safe Computing Survey Key

Score each survey from zero (low) to 54 (high). *(Find a sample survey key on page 4.)* Average these scores to get a quick metric of how your organization is doing as a whole. If you collected names and can do an “apples-to-apples” comparison of how individuals’ progress has improved over time, even better. And if you need help crunching your data, reach out to UD’s Center for Cybersecurity and Data Intelligence at udaytoncyber@udayton.edu.

This publication is a public service of the Ohio Department of Education, the Ohio Cyber Range Institute, and the University of Dayton Center for Cybersecurity and Data Intelligence.

Let’s Go Surveying

1

Conduct a pre-survey

Before you begin the training program, ask your colleagues to complete the survey. This will give you a baseline measure of where your organization stands before training.

Ask the respondents to include their name on the survey so you can reach out to them directly when you distribute the Post-Survey. Being able to match the “before and after” for several individuals will help you better determine how effective the training was.

2

Apply some training

Once you’ve collected responses from your pre-survey, it’s time to get to work. Distribute the monthly Becoming Cybermindful newsletters, provide some phishing practice, maybe even host some in-person activities.

3

Conduct a post-survey

After you’ve applied a good dose of cybermindfulness training (we recommend a full year, but give it at least 6 months), ask your colleagues who completed the pre-survey to provide their feedback on the post-survey.

In addition to the base questions below, you can also use the post-survey as an opportunity to get your colleagues’ opinions on the training overall—did they think it was helpful? What did they find most valuable? And least valuable? These answers will help you improve your cybersecurity training efforts going forward.

4

Compute your results

Once surveys are completed, compare your “pre” and “post” responses to see what kind of progress your organization has made. The Safe Computing Survey Key at the end of this document offers a quick way to score answers.

5

Share your results with us!

If you’ve gone through the trouble of surveying your users, our team of cybermindfulness aficionados at the University of Dayton would love to hear about it. Share your results with UD’s Center for Cybersecurity and Data Intelligence at udaytoncyber@udayton.edu. Your feedback will help us develop more resources you can use in the future!

Name: ______________________________ Date: ____________________

Safe Computing Survey

Thank you for participating in this Safe Computing survey. Your responses will help us improve the quality of our safe computing training. Remember there are no right or wrong responses; just reflect on the question for a moment and answer it.

The chances of receiving an email that contains a virus or directs you to a phony website is very small.
Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree

I rush through my email without being attentive to what the sender is asking me to do.
Never | Rarely | Often | Almost Always

Cybersecurity is something that we practice to protect ourselves and others.
Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree

I have a responsibility to protect my computer from hackers to ensure that information stored by other people remains secure.
Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree

I am confident that I would recognize a suspicious email message.
Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree

I wouldn't enter personal information online without verifying the site was legitimate.
Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree

If I realized I'd been victimized by a phishing exploit, I would notify my organization's IT support team immediately.
Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree

I would not open an attachment in an email from someone I did not know.
Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree

I use a different password for all of my important online accounts.
Never | Rarely | Often | Almost Always

My actions online can put my organization's data at risk.
Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree

I have a responsibility to protect my organization's information resources.
Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree

I would recognize a suspicious email message.
Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree

I think 2-factor authentication is an important security measure.
Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree

I update the software and apps on my computer and other devices.
Never | Rarely | Often | Almost Always

If I receive an unexpected link or attachment, I open / click it to see what it is.
Never | Rarely | Often | Almost Always

Safe Computing Survey Key

The chances of receiving an email that contains a virus or directs you to a phony website is very small.
Strongly Disagree (4) | Disagree (3) | Neutral (2) | Agree (1) | Strongly Agree (0)

I rush through my email without being attentive to what the sender is asking me to do
Never (3) | Rarely (2) | Often (1) | Almost Always (0)

Cybersecurity is something that we practice to protect ourselves and others.
Strongly Disagree (0) | Disagree (1) | Neutral (2) | Agree (3) | Strongly Agree (4)

I have a responsibility to protect my computer from hackers to ensure that information stored by other people remains secure.
Strongly Disagree (0) | Disagree (1) | Neutral (2) | Agree (3) | Strongly Agree (4)

I am confident that I would recognize a suspicious email message.
Strongly Disagree (0) | Disagree (1) | Neutral (2) | Agree (3) | Strongly Agree (4)

I wouldn't enter personal information online without verifying the site was legitimate.
Strongly Disagree (0) | Disagree (1) | Neutral (2) | Agree (3) | Strongly Agree (4)

If I realized I'd been victimized by a phishing exploit, I would notify my organization's IT support team immediately.
Strongly Disagree (0) | Disagree (1) | Neutral (2) | Agree (3) | Strongly Agree (4)

I would not open an attachment in an email from someone I did not know.
Strongly Disagree (0) | Disagree (1) | Neutral (2) | Agree (3) | Strongly Agree (4)

I use a different password for all of my important online accounts.
Never (0) | Rarely (1) | Often (2) | Almost Always (3)

My actions online can put my organization's data at risk.
Strongly Disagree (0) | Disagree (1) | Neutral (2) | Agree (3) | Strongly Agree (4)

I have a responsibility to protect my organization's information resources.
Strongly Disagree (0) | Disagree (1) | Neutral (2) | Agree (3) | Strongly Agree (4)

I would recognize a suspicious email message.
Strongly Disagree (0) | Disagree (1) | Neutral (2) | Agree (3) | Strongly Agree (4)

I think 2-factor authentication is an important security measure.
Strongly Disagree (0) | Disagree (1) | Neutral (2) | Agree (3) | Strongly Agree (4)

I update the software and apps on my computer and other devices.
Never (0) | Rarely (1) | Often (2) | Almost Always (3)

If I receive an unexpected link or attachment, I open / click it to see what it is.
Never (3) | Rarely (2) | Often (1) | Almost Always (0)