Strategies for assessing cybersecurity awareness training effectiveness

OMDIA

Brought to you by Informa Tech

Contents

Introduction

Measurement without meaning is wasted effort. In too many organizations, cybersecurity awareness training is viewed by top executives as an expensive exercise in ticking off a box in the “due diligence” column and not as something that has a material impact on risk reduction. Properly assessing the impact training has on employee behavior can be a major step in changing that view.

The best assessments of cybersecurity awareness training have a well-considered beginning, an ongoing basis, and a delivery mechanism with meaning for the greatest number of stakeholders in the organization. Properly assessing the effectiveness of delivered training will provide critical insight into the organization’s current risk status and an important guide to training programs in the future.

Know why you measure

"Why" is the first question

Measuring results is not a hard sell in business, but understanding what you will do with the results—the "why" of measuring cybersecurity awareness training results—can inform decisions on precisely what is measured and how it is analyzed.

- **Performance**: Are your employees learning the lessons being taught? This is the most basic measurement in training.
- **Application**: Can your employees do meaningful things with the lessons they've learned? You want to know that lessons translate to the real world.
- **Retention**: You'll measure performance or application of lessons after time has passed to see whether employees retain the training or need refreshers.
- **Investment**: This measurement is to determine whether the organization's investment in training is producing the intended results. The primary audience for this type of measurement is the executive board—results must be in a language they can use.
- **Risk Reduction**: Is your cybersecurity awareness training program specifically part of your risk reduction strategy? If so, then measuring results in ways that readily translate into risk metrics is critical.
- **Regulatory Compliance**: Regulations can have very specific requirements when it comes to topics covered in training.

If you don't know why you're measuring training results, you're likely to get fuzzy metrics that aren't perfectly suited for any particular analysis. When you go into the process with a specific requirement in mind, you can generate metrics that allow precise analysis that more comprehensively meets the company's needs.

Risk is the common language

When any training is measured, those measurements must be expressed in language that means something. For a growing number of organizations, that language is risk. Whether the initial focus of the assessment is measuring lesson retention or investment effectiveness, translating the results into a risk metric allows them to be shared with a wide range of stakeholders.

Risk metrics are used directly by many within organizations and are readily translated into the *lingua franca* of business: money. When changes in risk can be stated in changes to financial outlook, they can be understood, analyzed, and acted upon across the company.

The greatest limitation of risk as a language for expressing training effectiveness is that there is no standard for how to describe risk. There are different standards and practices, each of which can be useful within an organization but difficult to use when benchmarking against other organizations and standards. This limitation shouldn't restrict risk's use as an essential language for assessing cybersecurity awareness training; it simply means that comparing your organization's risk to others in your industry may require an additional level of translation.

More data makes for better assessment

One of the most dangerous things to do with any data analysis is trying to make too broad a conclusion from too small a data set. And many organizations will try to draw sweeping conclusions about the state of employee training from a single training encounter. Don't do that.

At best, data based on a single training encounter can tell you about the initial employee response to that encounter. If you want to draw more accurate conclusions about the state of employee training, you're going to need multiple data points gathered over time.

In many cases, organizations will employ a training strategy that involves lessons delivered on a regular, ongoing basis. This strategy lends itself to assessments that accompany each lesson—assessments that can cover not only the most recent lesson but previous lessons also.

Once a number of assessments have been taken, more reliable conclusions can begin to be drawn about both the success of the training method and the general level of organizational training. Drawing conclusions about either based on a single training session delivered once a year is like predicting the weather based on an annual glance at the thermometer: The accuracy of the conclusion is likely to be lacking.

Bottom line

- Training employees to recognize and properly respond to cybersecurity threats is neither optional nor a luxury in today's threat environment. As with any business necessity, it makes good business sense to know how effective the effort is and whether the investment is bringing the greatest return.
- In order to get the most useful testing results for the organization, you must begin by knowing precisely what it is you're testing for, and the use to which you'll put the analysis. While good data can serve multiple purposes, fuzzy thinking at the beginning of the process is likely to lead to less accuracy and utility at the end of the process.
- If you want to make the broadest use of the assessment results and share the information most widely within the organization, then translating the data into the language of risk is necessary. Risk reduction is a goal for most businesses, and the direct translation of risk posture into financial results makes risk a language understood both across and up and down the organization.
- The best and most useful method for assessing the effectiveness of your cybersecurity awareness training will involve regular testing to measure its impact on employee behavior. Behavior modification is the goal for all cybersecurity training, and employee behavior is a dynamic, constant factor in the company's risk level and response to cybersecurity threats. Watching that behavior change, measuring its dynamics, and mapping the results to the lessons that have been taught will provide the most accurate, useful insight into just how effective the training has been and be the most useful roadmap for training in the future.

To learn more

Watch this free webinar

Measuring effectiveness in security awareness training

presented by Omdia and our partner

CYBEREADY THE HUMAN READINESS COMPANY

The webinar can be accessed at:

https://bit.ly/3CScpxq

For additional Omdia events, visit:
https://gateway.on24.com/wcc/eh/753397/Omdia+Webinars

Follow the conversation @OmdiaHQ

Author

Curtis Franklin
Senior Analyst, Enterprise Security Management
curt.franklin@omdia.com

Get in touch

www.omdia.com
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the “Omdia Materials”) are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together “Informa Tech”) and represent data, research, opinions or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness or correctness of the information, opinions and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees and agents, disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial or other decisions based on or made in reliance of the Omdia Materials.