FORTRA™

GUIDE (TERRANOVA SECURITY)

The Power of Personalized Reporting in Security Awareness Training

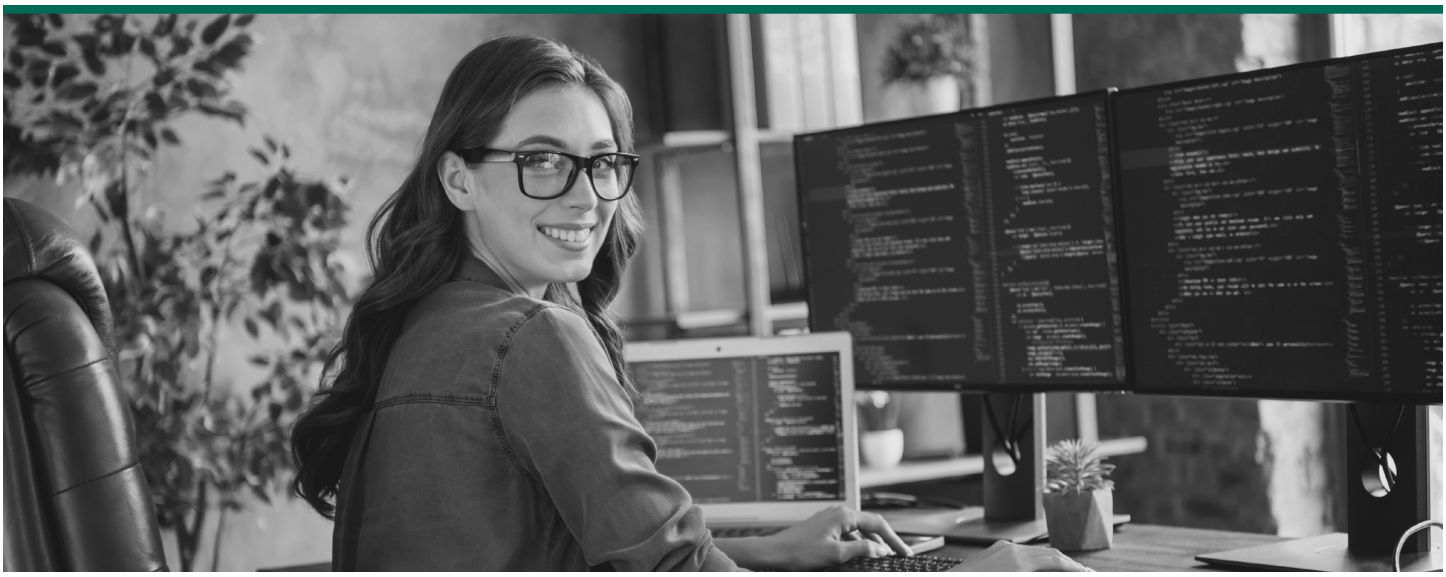
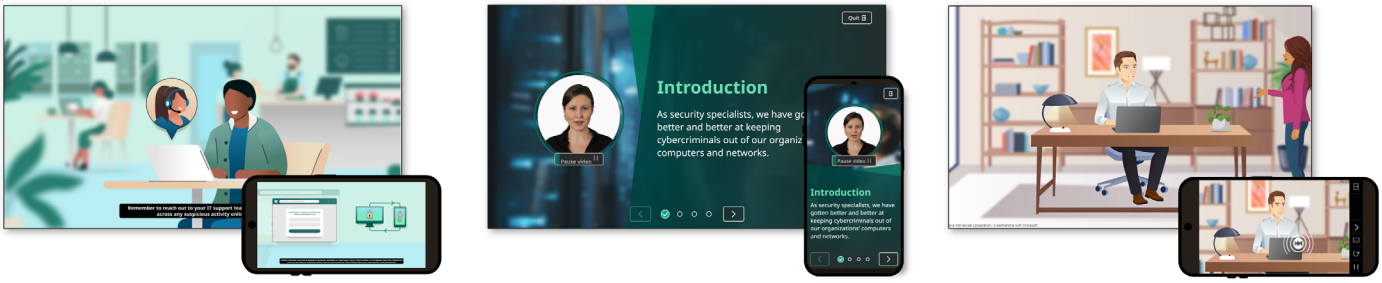


TABLE OF CONTENTS



INTRO

A robust, multifaceted training program that evolves over time is only as good as the data that drives it. To that end, what separates basic analytics from actionable data-driven insights is how personalized they are to your organization's overall strategy.

High-level data points, like the total number of users who've started or completed a training course, will only give you a general impression of performance. In other words, does knowing that 60% of employees have finished a particular course empower organizational leaders to make informed decisions that will help them train strong, effective cyber heroes?

The answer to this question becomes more complicated when applied to a larger, possibly more distributed workforce. As a result, the degree of decision-making difficulty without information that supports specific strategic goals increases exponentially.

To facilitate security awareness optimization and innovation, your analytical viewpoints must be customized to deliver the information you need to succeed. This level of personalized reporting, including consideration for different geographic regions or departments within an organization, offers clear insights that align with quarterly or yearly cyber security goals.

Specific, relevant analytics also allows you to tap into your data's full potential with more detailed performance breakdowns related to courses, simulations, and related initiatives. Most importantly, customized reporting enables your organization to tailor data visualizations to its specific needs.

> **Your goals and strategy will differ from other organizations in your industry, region, or size bracket. They'll also evolve over time.**
>
> **So why settle for out-of-the-box reporting that doesn't consider that reality?**

The Difference Between Generic and Personalized Reporting

Taking an in-focus snapshot of your training program's effectiveness with generic reporting data is a reality that many cyber security and business leaders face, especially in an era of accelerated digital transformation. However, since global statistics can only draw insight from a high-level vantage point, an organization's long-term security awareness performance will be at the mercy of those restrictions.

Reporting that delivers actionable, powerful security awareness training analytics goes far beyond static pass/fail-style metrics. Instead, they allow you to tailor different dashboards to suit your needs and, through personalization, extract the right information at the right time.

Access to customizable reporting enables you to get very granular about what you measure. Having various filters and parameters helps pinpoint data about specific training courses, simulations, custom filters, and more. As a result, your organization can focus on finite campaign issues and tie them to larger training programs or business objectives.

Without this level of personalized reporting, targeting the right user behaviors and benefitting from a meaningful reduction in information security risk is far more complicated.

In short, generic analytics borne of basic reporting tools offer cyber security and other business leaders about as much detailed insight as looking out an airplane window. You'll be able to spot some major landmarks, but that's about it. Seeing city streets, architecture, or other smaller details is extremely difficult, if not impossible.

Terranova Security Pro Tip

For your data to be an asset, it must be finely tuned to your organization's goals and the underlying strategy fueling your progress.

How Data-Driven Insights Unlock Security Awareness Training Success

In today's business climate, where accelerated digital transformation is the norm, detailed data-driven insights are key to unlocking your security awareness training program's full potential.

Recent studies show that highly data-focused organizations are three times more likely to report improved decision-making. This kind of optimization doesn't happen by accident either. Reporting on the right metrics and extracting the most accurate insights possible is a critical part of any initiative.

To properly support user behavior change and, over time, help keep sensitive personal and organizational information safe, your security awareness training analytics must be:

SPECIFIC

Your dashboards need to rely on specific parameters (e.g., a particular course or simulation, geographic region, or department) to extract and display pertinent analytics that drives your reporting.

UP TO DATE

Ideally, your analytics platform should be capable of delivering real-time updates that reflect the most recent user actions.

GOAL-ORIENTED

Every piece of data you collect must serve your security awareness training program's global strategy, as well as any related business goals. These unique, actionable realities need to be reflected in your analytics.

The nature of cyber threats is constantly changing. Therefore, using the data at your disposal is vital to shaping a cyber-secure future for your organization.

Terranova Security Pro Tip

Optimization is part of the Terranova Security 5-step security awareness training framework, which helps organizations maximize their cyber security investment in their end users.

Building a Personalized Reporting Dashboard: Where to Start

If your organization is just starting on its security awareness training journey, or if your current analytics and reporting framework are yielding unsatisfying results, it can be challenging to know where to begin.

Which metrics should you target with your reporting dashboards? How do you ensure that you're extracting insights that are accurate, relevant, and consistently supporting your information security initiatives?

When you create a personalized reporting dashboard, it's important to start with your training program's foundational elements and build your analytics hub out from there. Start with your overall strategy and ask yourself the following:

- Which user behaviors is your organization targeting with training courses and phishing simulations?
- Of those behaviors, which ones are tied to your biggest security awareness training priorities?
- Which initiatives will you/have you launched that directly support those priorities?
- What are the goals for each initiative (e.g., training course, simulation, ongoing campaign)?
- Concerning those goals, what metrics are most critical in determining each initiative?

By linking specific metrics to each aspect of a security awareness training program, your organization's leadership team can instantly quantify monthly or quarterly progress towards achieving your cyber security goals. As your programs grow, evolve, and even multiply over time, it will be easier to adjust the reporting dashboard layout accordingly.

Terranova Security Pro Tip

Optimization is part of the Terranova Security 5-step security awareness training framework, which helps organizations maximize their cyber security investment in their end users.

Building a Personalized Reporting Dashboard: Key Components

When customizing your security awareness training reporting, understanding the key components of your program is essential. With a firm grasp of this information, you'll be able to efficiently structure your analytics and extract all the vital training program data points.

Regardless of your organization's size or the industry it operates in, Terranova Security recommends including reporting dashboards that cover the following components:

Security Awareness Training Courses

Construct dashboards that enable you to drill down and distill important course information into granular, actionable observations.

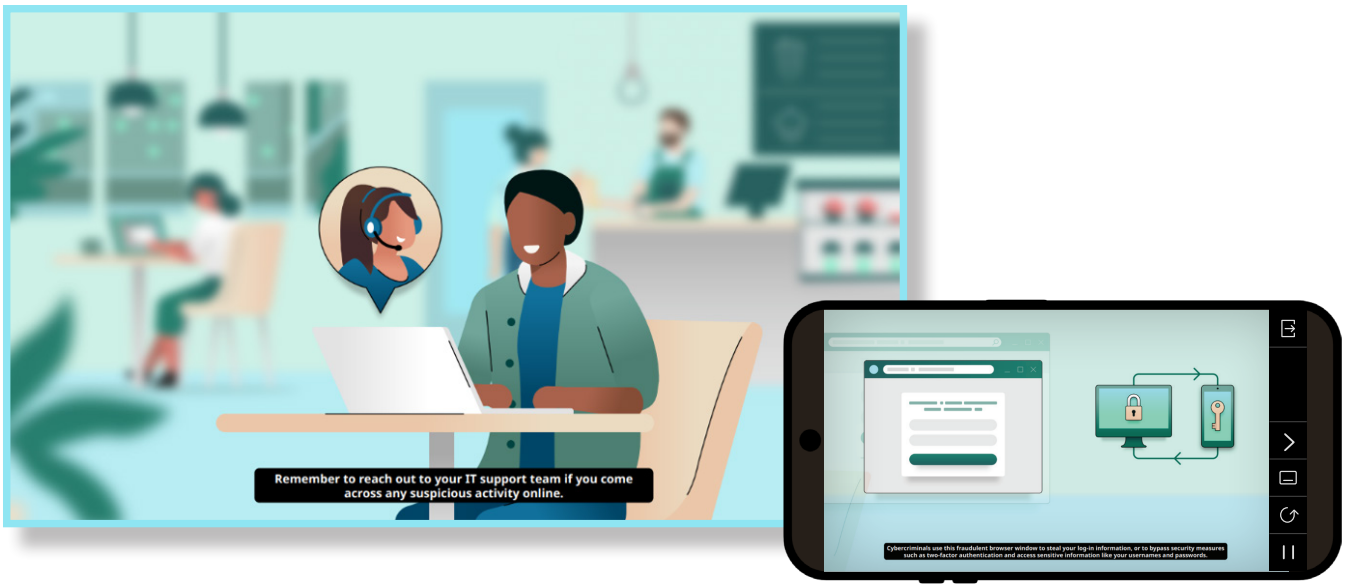
Filtered Data Breakdowns

Ensure that your leadership team can filter their data breakdowns using dashboard analytics based on region, department, user progress, and more.

When selecting each component of your reporting dashboard, make sure you choose the right visualization style to match the type of data being represented. Also, consider which stakeholders will view the information and select the visualization accordingly.

Terranova Security Pro Tip

You can stylize different data segments differently, such as utilizing a bar instead of a pie chart or a line graph, in the Security Awareness Platform to ensure clear, concise visualization and communication.



Building a Personalized Reporting Dashboard: Next Steps

Once you have an initial reporting dashboard set up and have ensured the data therein is accurate and up to date, it's time for the next phase: optimization.

Your organization's security awareness training hub must grow and evolve alongside your training programs and your overarching cyber security goals. As such, each dashboard and widget must reflect major changes to your security awareness program's key components.

Terranova Security recommends creating a short checklist your organization can regularly use to ensure you're always getting the most out of your reporting data.

- Are any new cyber security goals or essential metrics not represented by a widget or dashboard?
- Of your existing reporting assets, is any data being collected no longer relevant or directly supporting a training initiative or goal?
- Is any of the data being collected too general, inaccurate, or incomplete?

Keep in mind that these questions are just a starting point and by no means an exhaustive list. The checklist itself should also be an evolving organism updated regularly alongside your security awareness training program. For increased reporting accuracy, make sure you sync with campaign stakeholders and ask them if they're getting the information they need.

Terranova Security Pro Tip

Clear, concise reporting is critical to security awareness training success. Assess and refine your reporting dashboards at least once per quarter by cutting any irrelevant information and ensuring that all data represented support your cyber security goals.

The Terranova Security Awareness Platform: Dashboards and Reporting

Get the customizable, granular reporting needed for better data-driven decision-making with the Terranova Security Global Dashboard and enhanced reporting capabilities.

Use the flexible, widget-based interface to build completely customizable reporting dashboards that display your most important security awareness training data.

With different visualization options and real-time data updates, you can capture specific training insights for your leadership team and use them to strengthen your organization's data protection.

The Terranova Security Global Dashboard centralizes your key analytics into one streamlined hub for seamless data collection and representation. As a result, finding and assessing crucial information about your security awareness training initiatives is always just a few clicks away.

Go beyond generic, one-size-fits-all reporting by getting granular insights that accurately reflect your security awareness training performance and accomplishments. With better data, you can quickly pinpoint improvement areas, easily tweak objectives, and instantly reduce related cyber security risk levels.

Details matter. Ensure that your organization has the right ones at its disposal with the Terranova Security industry-leading training solution.

Book a personalized demo today!

Find out more about the Global Dashboard feature and why it's indispensable for growing and optimizing your security awareness training program.

REQUEST DEMO

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.