proofpoint.

E-BOOK

Measuring Security Awareness Impact for Long-Term Success

A Guide for CISOs and IT Leaders

85%

of U.S.-based CFOs reported that their boards have had a formal discussion about recent cybersecurity attacks and the aftermath of the events.[1]

Introduction

For IT and security leaders, the nascent decade has been a whirlwind of challenges and change. From the pandemic-fueled scramble to connect remote workers to a surge of phishing attacks seeking to exploit the chaos, 2020 was only the start of a daunting new era for cybersecurity.

In a recent survey of tech professionals, 57% said their organisation dealt with a successful phishing attack in 2020, up from 55% the year before.[2] And the barrage isn't letting up. A growing surge of high-profile ransomware and data breaches is forcing companies to reckon with their appetite for risk.

Compromise is painful for victims. But it can spark much-needed conversations among executives and the board about cybersecurity and the role user behaviour plays in safeguarding the business.

Most cyber threats require humans to activate them. That's why effective security awareness programmes—and changes in user behaviour—can play an outsized role in reducing risk.[v] Many security leaders know this intrinsically. But measuring—and communicating—the impact of your security awareness programme to executives doesn't always come as naturally.

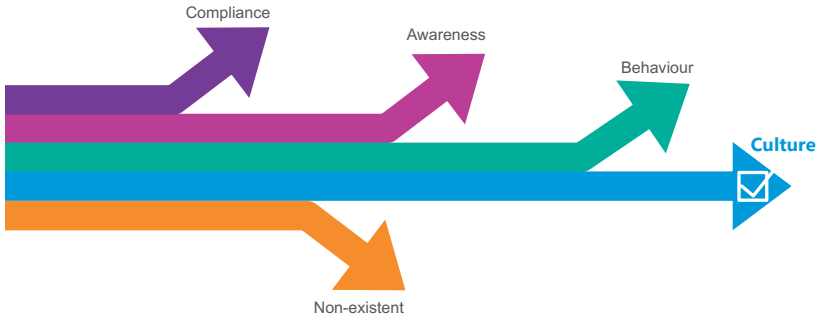
This e-book explores in the ins and outs of security awareness programmes built for long-term success. It outlines strategies for championing, measuring and nurturing stakeholder buy-in. And it shows you how to make the most of this critical investment.

[1] CNBC. "CNBC Global CFO Council Survey." July 2021
[2] Proofpoint. "2021 State of the Phish." February 2021
[3] Proofpoint. "Protecting the End User." February 2019

The State of Security Awareness

Security awareness tends to be a lower budget priority than technical controls. But it doesn't have to be. With compelling metrics and an effective narrative, you can achieve two key goals. First, you can tangibly reduce risk. And just as important, you can show CISOs and other stakeholders why security awareness is such a critical tool in the organisation's security toolkit.

Upper management's concerns will hinge on the state and goals of the existing security programme. Compliance-driven programmes, for example, will focus on checking boxes to meet standards. Behaviour-based programmes, on the other hand, will measure success based on metrics like click rate and reporting rate on phishing simulations.



Stages of maturity for security awareness programmes

Pathway to establishing a security culture

Most organisations (98%) have a security awareness training programme.[4] Yet, 64% of them conduct only formal training sessions (either in person or virtually)—missing other opportunities for security awareness enrichment. Only 23% use a mix of all available assessment, education and communication media.

Continuous and ongoing engagement through a variety of channels will improve retention and security awareness outcomes. That's why we strongly recommend using as many channels as possible.

A key tenant to better security awareness is building a culture where users believe that strong security is good for not just the organisation, but for them personally. You can achieve this by blending activities to drive awareness, change behaviour and instill a dedication to "fighting the bad" for the greater good. That means making training relevant and useful for users—continuously, not just once or twice a year.

Current approaches to security awareness:[5]

29% strictly use simulated phishing tests

41% strictly use formal training sessions

7% strictly use informational content

23% use a mix of content types

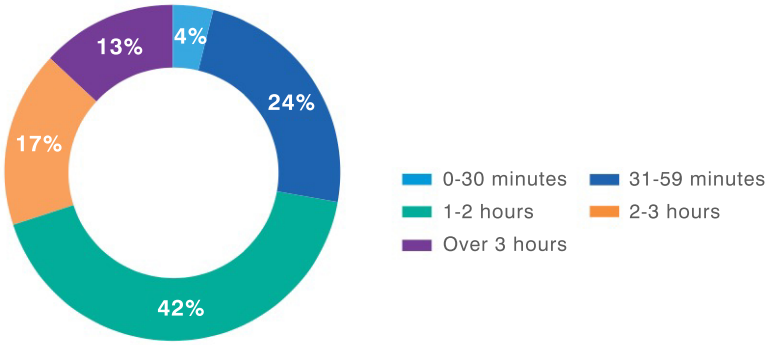
[4] Proofpoint. "2021 State of the Phish." February 2021
[5] Ibid.

How to Run a Programme that Makes an Impact

The more time an organisation invests in its security awareness efforts, the better chances of success.

Time Organisations Dedicate to Security Awareness

Most organisations have less than two hours per user per year to make an impact.



Every year more organisations increase the frequency of security awareness activities.

Focus engagements on vulnerable users

Sometimes, you may face resistance when trying to expand your security awareness programme. Skeptics may fear that the programme will burden too many users, especially those who don't pose a high risk.

Focusing on vulnerable users at a more frequent cadence, rather than a blanket approach that imposes more training on everyone, can help allay some concerns. With a targeted approach, stakeholders know there is a good reason for added training sessions and security awareness efforts. And users have context for why they're receiving it.

Others may be concerned less about the number of people affected than with the amount of time training takes. Fortunately, you can bolster awareness in ways that don't waste users' time.

Consider newsletters, townhalls, wiki pages and email notifications for time-efficient security awareness.

Do You Know Who Your Most Vulnerable Users Are?

At Proofpoint, we use the term Very Attacked People™ (VAPs) to describe the category of users that cyber attackers target with unusual intensity. This might involve high volumes of attacks, narrowly targeted threats, advanced tactics—or all three. While all users are targets, VAPs are prized for their unique professional contacts and privileged access to data, systems and other resources.

VAPs are **3-12X** more attacked compared to other users

We have found that VAPs are not always an organisation's VIPs, such as senior executives. They can be part of the human resources, public relations, marketing or research teams. Anyone with the right access can be a high-value target.

Once you've identified VAPs, closing the security knowledge gap with hyper-targeted education is crucial. For instance, consider sending VAPs targeted by credential phishing simulated phishing attacks. If they fall for the simulation, offer optional education. This sequence is a targeted way to reduce known people-based risk without wasting users' time.

Security awareness is not a one-and-done process. You need comprehensive, ongoing education that keeps pace with the cyber threats your users are facing. This process includes:

- Regular assessments
- Education
- Reinforcement activities
- Measurement

To stay on-track and align stakeholders, consider creating a schedule outlining activities, channels, messages, and themes for your programme.

Measuring Security Awareness Excellence

Many programmes measure success based solely on completed training sessions (for compliance) and the rate at which users fall for simulated attacks. But to truly change user behaviour and reduce risk, you must move beyond these activities.

You can go a level deeper with more complete user-risk profiles. Here are key measurements that help quantify real security impacts:

Reporting rate of simulations

This metric provides insight into end users "avoiding the bad," but even more noteworthy—"doing the good." That means putting their security awareness training into action when they spot something suspicious.

Real click rate

Proofpoint Advanced Email Security lets you to see the click rate of actual unsafe content even if the URL is blocked or rewritten for security purposes. This metric peels back the curtain to reveal users' real-world knowledge. With this data, you can track whether users are getting better at spotting real unsafe content.

Reported message types

Using an email add-in, users can report suspected malicious content, much like they do with an abuse mailbox. Proofpoint Targeted Attack Protection (TAP) shows you how it classified various types of email (malicious, spam, low risk, and so on). You can see users are getting better over time at reporting messages that could harm the organisation.

Real Impacts

This is the most important measurement of all. The Real Impacts metric tracks what users are actually doing—whether you are dealing with fewer successful phishing attacks, credential compromises, insider incidents and malware. That's the ultimate measure of excellence. What's more, it is key to getting long-term buy-in for security awareness programmes.

Answering the question: Where should we be for click rate and reporting rate?

Proofpoint recommends:

<5% failure/click rate

>70% reporting rate

Communicating Effectively to Your CISO and Key Stakeholders

When reporting to leadership and stakeholders, fear, uncertainty and doubt (FUD) gets you only so far. Yes, cyber threats must be managed. But when scare tactics are overused and threats are exaggerated, you may create a classic “boy who cried wolf” scenario that does more harm than good.

Key ways to communicate security awareness performance

Quantitative

Context matters. That’s why understanding your overall performance and how you compare against others is critical. When benchmarking against peers, focus on positive metrics rather than negative ones such as simulation click rate.

Positive metric examples include:

- Increases in user reporting rates for simulated phishing emails
- Improvements in security awareness knowledge assessments
- Accuracy gains in user-reported actual malicious messages
- Greater user-participation rates in security awareness activities

Qualitative

Combined with data, stories can help build a narrative that security awareness is more than a required compliance activity. These narratives help show how users’ behaviour is changing; that the culture is actively shifting as users understand risks; and that the effort is helping to protect the company.

Narrative examples:

- A user stopped a real, sophisticated phishing attack
- Users expressed positive sentiments about the awareness programme in a feedback survey
- An executive staff member or well-known person shared something about security awareness to their staff

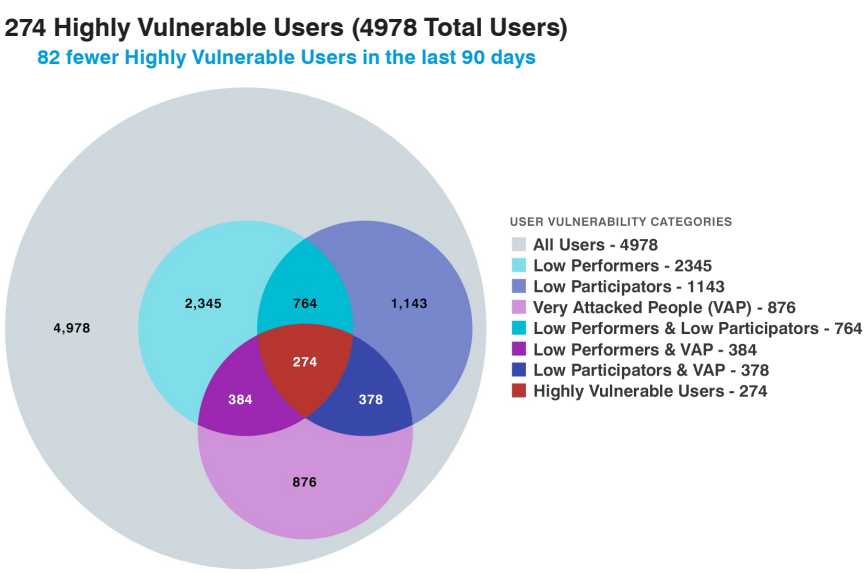
Security Awareness Clarity in a Dashboard

Security awareness is one of the most important things you can do to protect your organisation. That's one of the reasons we built a CISO Dashboard for Proofpoint Security Awareness. Using the dashboard, IT and security teams have access to key metrics that prove security programmes are changing behaviour and driving culture. Armed with these measures of success, the ROI—and argument for future investment—becomes much more obvious.

With the Proofpoint CISO Dashboard, you have access to metrics that include user vulnerability and your security programme score.

User Vulnerability

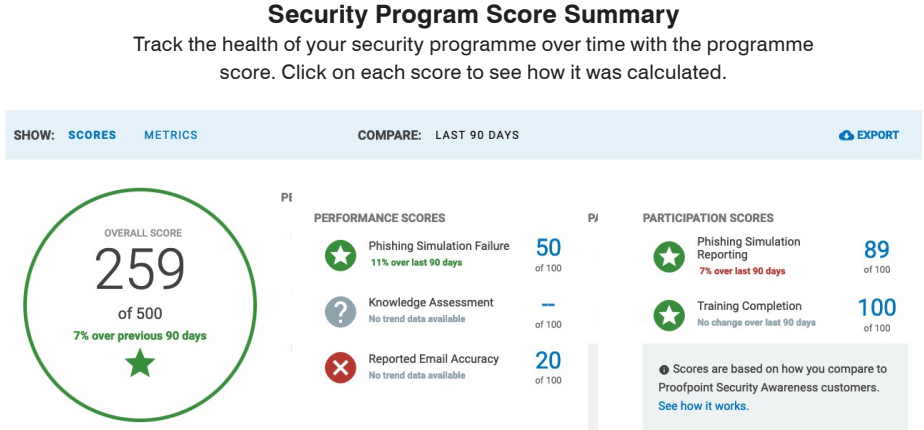
See low performers and participators along with those clicking on real malicious messages. If users are VAPs in Proofpoint Targeted Attack Protection, that data is integrated for a better view of that user's overall risk profile.



The User Vulnerability Summary in CISO Dashboard

Security Program Score

Performance and participation score show the percentile ranking of your organisation in each area and how the overall score has changed. With stoplight-style icons, you can know where you stand in each area at a glance and see opportunities for improvement.



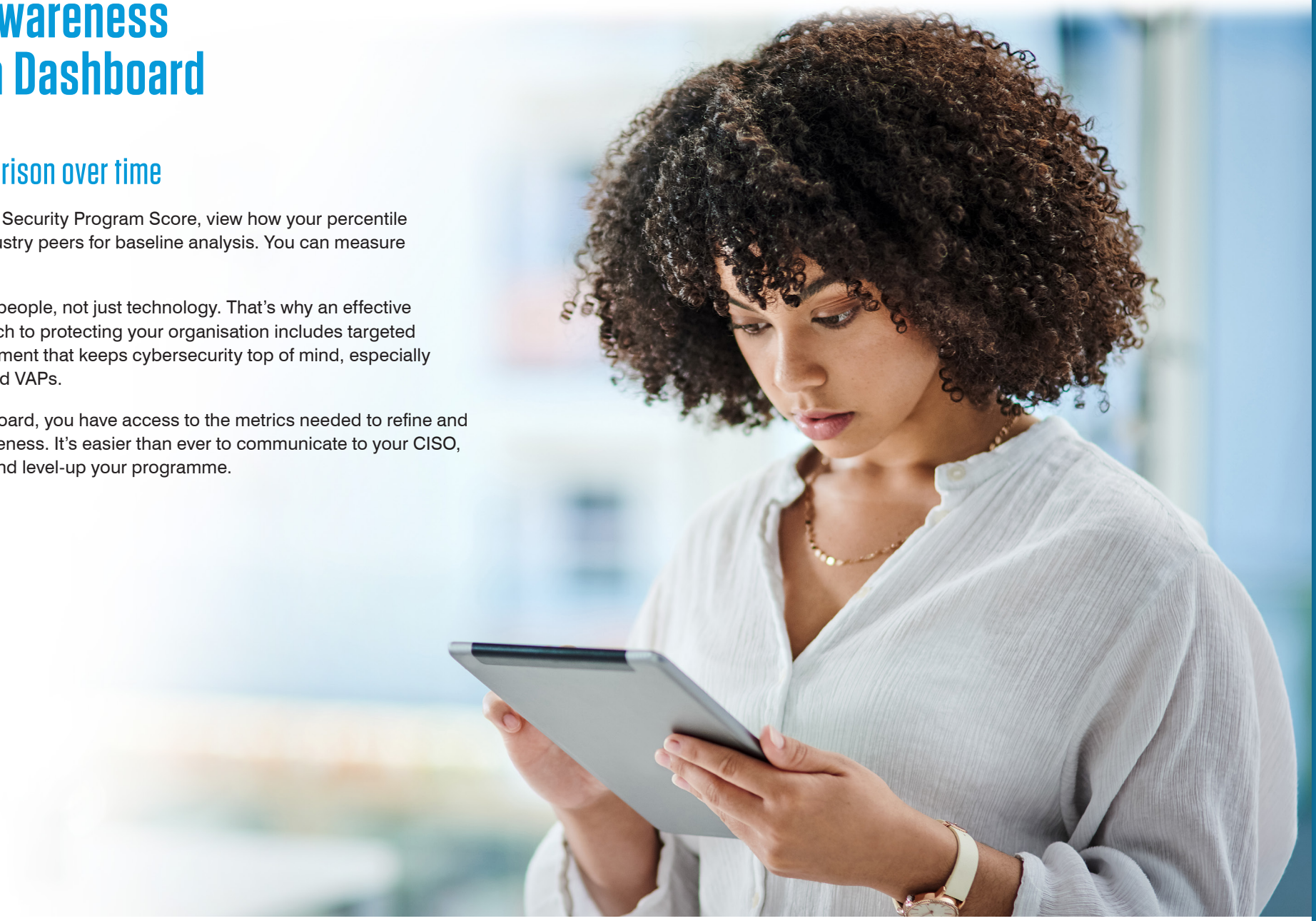
Security Awareness Clarity in a Dashboard

Percentile comparison over time

In conjunction with the Security Program Score, view how your percentile compares to other industry peers for baseline analysis. You can measure progress over time.

Today's attacks target people, not just technology. That's why an effective people-centric approach to protecting your organisation includes targeted education and engagement that keeps cybersecurity top of mind, especially for vulnerable users and VAPs.

Using the CISO Dashboard, you have access to the metrics needed to refine and advance security awareness. It's easier than ever to communicate to your CISO, get continued buy-in and level-up your programme.



To learn more about how Proofpoint can help you change user behaviour and make cybersecurity a core element of your corporate culture, visit proofpoint.com.

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organisations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyber attacks. Leading organisations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at **www.proofpoint.com**.

proofpoint.

0504-002-01-01 09/21