E-BOOK

Beyond Awareness Training

Building a sustainable security culture—and why it matters

proofpoint.

Introduction

By now, most cybersecurity leaders know that people are their organisations' biggest attack surface. Remote and hybrid work, coupled with a shift to the cloud, has only complicated this challenge.

According to the "2021 Verizon Data Breach Investigations Report (DBIR)", 85% of breaches involved the human element—whether triggered by users clicking on a malicious link in a phishing email or sharing credentials outside the corporation.[1]

Indeed, a recent Proofpoint survey shows that 75% of CISOs in the U.S. and 58% of CISOs around the world agree that human error is their biggest security vulnerability.[2] These days, anyone can be a target—and anyone can hurt their organisation's security posture.

To educate their users, and with the best intentions, many organisations provide one or two hours of security awareness training annually. But this limited approach lacks staying power. It doesn't promote lasting changes in behaviour. And it doesn't instill the kind of security mindset that can transform your biggest attack surface into a critical layer of defence.

[1] CISOMAG. "Verizon 2021 DBIR: Cyberattacks Continue to Rise During Pandemic." May 2021.
[2] Proofpoint. "2021 Voice of the CISO." May 2021.

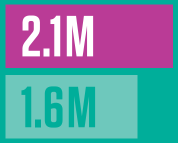
About 95% of organisations say they provide phishing awareness training to their users. But 30% say they train only portion of their user base.[3] It's no wonder that phishing is still the threat type most likely to cause a data breach.

What can we do better? The answer lies in developing a systematic, sustainable and customised security culture—one that pervades the organisation across all users and all digital activities.

This approach takes a concerted investment of time, effort, resources and companywide support. But the return can be invaluable. A robust security culture can improve your organisation's security posture, compliance and business outcomes. Done right, it can even boost employee morale and productivity.

of organisations around the world experienced a phishing attack in 2020, and 74% of attacks targeting U.S. businesses were successful.[4]

faced spear phishing. Highly targeted business email compromise (BEC) attacks are the second-most common form of social engineering. BEC attack volumes 15 times higher in 2021 than the year before.[5]



Google registered 2,145,013 phishing sites as of Jan. 17, 2021—up 27% from 1,690,000 on Jan. 19, 2020.[6]

[3] Proofpoint. "2021 State of the Phish." January 2021.
[4] Ibid.
[5] Verizon. "2021 Data Breach Investigations Report." July 2021.
[6] Chuck Brooks (Forbes). "Alarming Cybersecurity Stats: What You Need to Know for 2021." March 2021.

SECTION 1

Defining a Security Culture

At Proofpoint, we subscribe to a definition of organisational cybersecurity culture outlined by Keman Huang and Keri Pearlson, researchers at the MIT Sloan School of Management. As they describe it, a security culture is “the beliefs, values, and attitudes that drive employee behaviours to protect and defend the organisation from cyber-attacks.”[7]

In other words, employees—all of your employees—are active agents in the defence of the organisation’s data, systems and resources.

[7] Keman Huang and Keri Pearlson (MIT). “For What Technology Can’t Fix: Building a Model of Organizational Cybersecurity Culture.” January 2019.

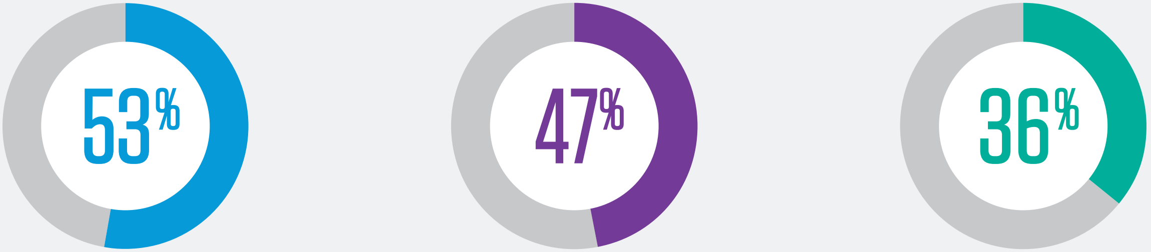
To build a security culture, you need to find ways to change how your people think about the topic. A security culture should be embedded into your core corporate culture. It must inspire—and endure.

What shapes a culture

A cybersecurity culture comprises three overlapping factors:

- **Responsibility for cybersecurity.** Employees feel that they and their coworkers are responsible for acting to prevent security incidents.
- **An understanding of why cybersecurity is important.** Employees believe that cyber threats are a material risk to the organisation's success and could affect them personally.
- **The power to act.** Employees feel empowered through their cybersecurity knowledge, understanding of security policy and trust that the organisation will support them if they make an honest security-related mistake.

In 2021:

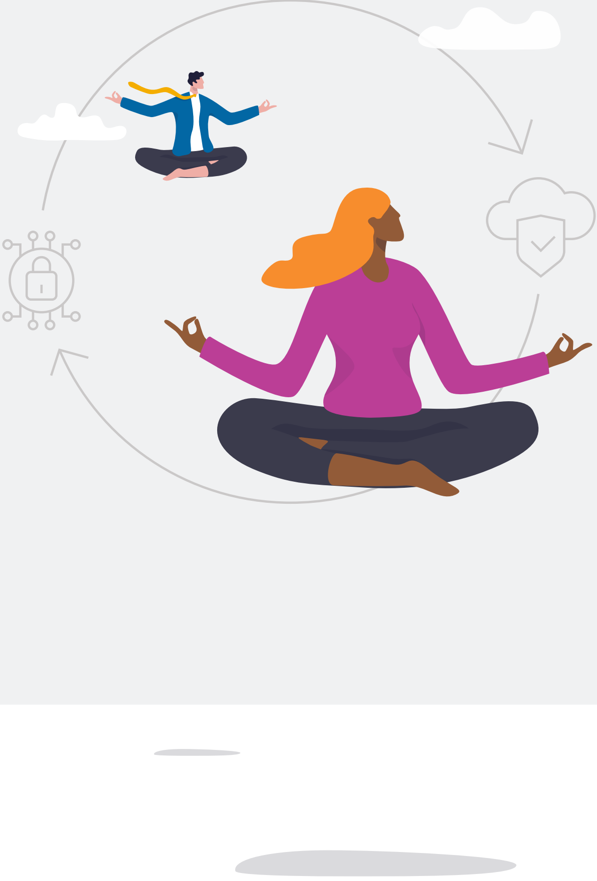


Just over half of all users could correctly define phishing

Nearly half of all users think all internal emails are safe

Just over a third of users could correctly identify ransomware

Source: Proofpoint. "2022 State of the Phish." January 2022.



Characteristics of a strong security culture

What does a security culture look like? Organisations are as unique as the people in them. And every industry sector is part of a larger subculture. Still, strong security cultures have a few universal characteristics. A strong security culture:

- **Is holistic and continuous.** A security culture needs to go beyond training or occasional phishing simulations. The goal is to raise morale and transform all employees to create a more engaged and secure workforce. You can achieve this in many ways. A security culture promotes learning and awareness through relevant and tailored content and updates on the evolving threat landscape. Users receive emails and other reminders that help employees understand why they are taking part in the programme and how it helps them at work—and in their personal lives. And they are encouraged to feel comfortable and confident about reporting suspicious digital events.
- **Has cross-functional advocates.** Support trickles down from the C-suite to management to end users. Apart from leadership, other champions may include security, information technology, HR, compliance and audit, and marketing and public relations.[8]
- **Creates and sustains expectations.** This involves devising and enforcing security policies that drive cultural norms.

[8] SANS Institute. “2021 Security Awareness Report: Managing Human Cyber Risk.” November 2021.

Creating a safe and just culture

An environment of psychological safety is foundational to a security culture. Security incidents can drag down any organisation, especially if someone is singled out as the cause. Employees sometimes see phishing simulations as punishing. They may feel inadequate or incompetent if they fall for the bait.

Create an atmosphere where employees feel comfortable about reaching out to the security team when they see something suspicious—and feel safe about letting security know about a slip-up.

Users also need assurance that pushing back is the right thing to do if asked to do something they know is insecure.

SECTION 2

The Challenges of Building a Security Culture

Organisations spend millions on security tools, services and staff. But even with those investments, many still overlook their biggest risk factor: people.

Tackling the human factor is the most important security measure you can take. It's also one of the trickiest. Awareness activities can seem disruptive and distracting. Some employees feel that it gets in the way of "real" work. Many resist the extra demands, such as reporting suspicious emails or sitting through training webinars. And technical staff and HR may feel timid about running a security culture because they are not equipped to build and nurture one.

Challenges include:

Selling the idea to upper management

Persuasively quantifying ROI

Convincing users that security training and awareness are positives and getting them to actively take part

Changing user behaviour

Overcoming obstacles

Few security leaders would dispute the value of security awareness. But achieving a strong security culture can seem daunting. Here are some of the obstacles you may face in the process—and how to overcome them.

Obstacle 1: Detractors in finance and operations

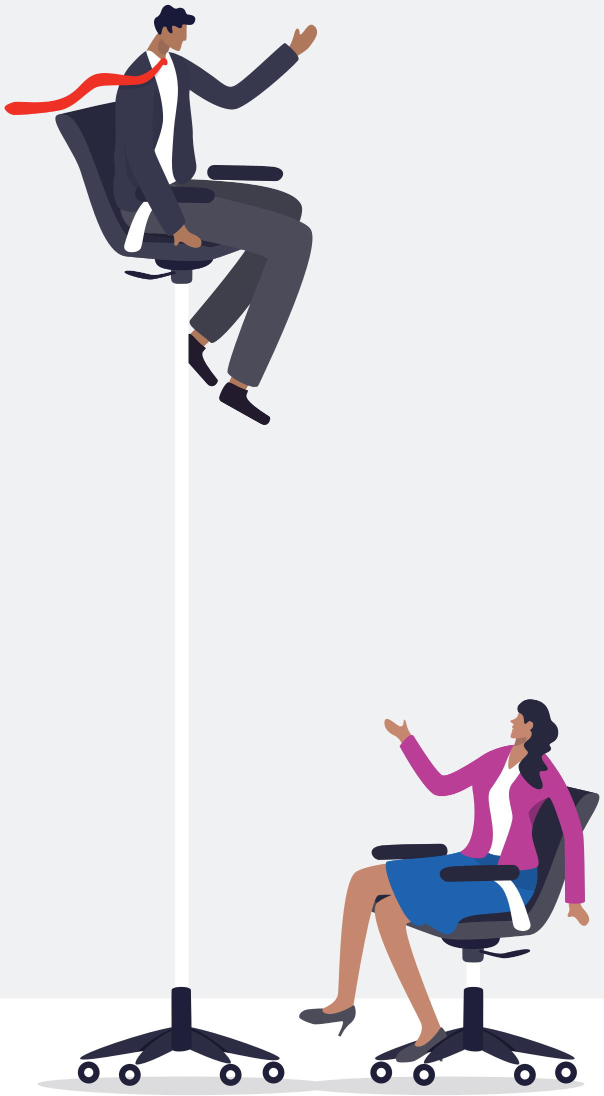
Your finance department may balk at the costs of funding security awareness programmes, especially if the organisation has already heavily invested in multiple security tools. At the same time, peers in operations may worry about a productivity hit because of training demands. The other two top issues cited by stakeholders are a lack of time and personnel to run the programme.[9]

How to respond: Justify the cost and effort

Speak the language of business. One way to build a financial case for a security awareness culture is to point out the cost of a breach ($4.24 million on average[10]) and compare that to the cost of training. At the same time, engaging operations can help. You'll get an opportunity to dispel fears of an oppressive user mandate. For instance, content delivered in micro learnings reduces training time while improving employee retention. Operations can also suggest ways to make the rollout smoother.

Gartner suggests that resource-strapped teams consider a managed security awareness training service to help launch and maintain the programme.[11] Service providers typically offer a subscription-based security awareness platform with dedicated services. These services may include scheduled phishing testing campaigns and other training.

[9] SANS Institute. "2021 Security Awareness Report: Managing Human Cyber Risk." November 2021.
[10] Ponemon institute. "2021 Cost of a Data Breach Report." August 2021.
[11] Gartner. "Market Guide for Security Awareness Computer-Based Training." September 2021.



Obstacle 2: Leadership reluctance

Like the finance department, the C-suite often sees security as yet another expense on the balance sheet. Leaders may feel that your organisation has already spent millions on tools and technologies and have little appetite for spending more.

How to respond: Communicate the true cost of unmitigated risk

One of the best ways to raise the awareness of executives is through tabletop exercises, such as mapping out what-if scenarios for common security incidents.

For example, give executives a play-by-play account of a ransomware attack. Show how easily an infection can take hold through a socially engineered email. Then, explain how the ransomware would lock up data and systems, all but shutting down business.

Fire drills can pack an emotional punch by showing what it's like to undergo a real attack. This helps the C-suite evaluate cyber risks and put them in context. It's a powerful way to drive home the importance of creating a security culture.

Showing which users in the organisation are most at risk—and why—can be effective for showing just how critical individual resilience is. (This effort is much easier with a modern security solution that can fuse vulnerability-, attack- and privilege-based risks into an easy-to-explain user risk score.)

You should also show how a security culture can offer a competitive edge. An effective culture builds trust and shows the market that the organisation cares about its customers, partners and employees.

You can strengthen your case by making core metrics—offered in a nontechnical and positive manner—part of your conversation with leaders.

78%

of organisations say security awareness training lowers susceptibility.[12]

Obstacle 3: User apathy and resistance

Driving change is always tricky. Trying to instill a whole new security culture can be even harder. Employees may wonder if they will be monitored. They may believe that security is not their job. Or they simply may not see any value in it.

Given that employees' time is one of the most valuable assets in a business, managers and executives may worry that security programmes will distract users and hamper productivity.

How to respond: Win hearts and minds

Again, present the effort in a positive light. Explain why a security mindset is important. Emphasise that training and reinforcement are by no means punitive. Instead, they allow for everyone to contribute to the safety, well-being and success of the company—and themselves.

Showing users their risk profile (perhaps including the score mentioned in the previous section) can help make things personal.

Share the headlines—real-life scenarios where the lack of security awareness led to serious threats that hurt productivity and resulted in major downtime.

Many of the security awareness skills employees learn in the workplace also apply to their home and family life. Framing the programme in a way that shows a security programme is personally valuable can help promote acceptance.

[12] Proofpoint. "2021 State of the Phish." January 2021.

Selling the benefits of a security culture

When explaining how a security culture can advance the organisation's mission, stick with meaningful, measurable benefits. Here are some that resonate with business leaders:

Improved agility and resilience. A security culture spurs employees to recognise potential threats. It also enables security teams to react to and resolve threats faster. Agility and resilience increase when users who are inspired, regularly engaged and supportive of each other achieve a network effect. The benefits ripple throughout the organisation.

Organisational risk reduction. We live in an era of remote and hybrid workforces, migration to the cloud, and increased use of personal devices. A strong security culture can put leadership's mind at ease—and let them focus on other areas of the business.

Pain-free compliance. Complying with government regulations, industry standards and internal security policies will become easier. That reduces the odds of fines and other penalties.

Competitive advantage. Customers and partners will choose your company over competitors when they feel that yours is safer to do business with. Promote security as a core value.

Hallmarks of a strong security culture

In a strong security culture, people have learned to be discerning. They have the tools, resources and knowledge to get the answers themselves. And they are encouraged to continually ask questions.

Actions, attitudes and beliefs define your security culture. These behaviours and mindsets are hallmarks of a well-developed culture:

If you suspect it, report it

Stop and think before you click

Have a secure mindset when working at home

Be discreet with private information

Regard information as a critical asset

SECTION 3

Making It Real: 3 Steps to Building a Security Culture

So, you're sold on the benefits of a strong security culture and your organisation is ready. Where do you start?

Motivation is the key to generating a strong security culture, and it involves three key ingredients. The first is **autonomy**. This means making learning personalised and self-directed for every user. The second is **mastery**. This means giving users the tools and time they need to progress and become proficient with cybersecurity knowledge and skills. And the final ingredient is **purpose**. This means giving users a sense that they're becoming part of a mission larger than themselves.

Here are three steps you can take to help you build a sustainable security culture. This is a continuous process that we call the ACE framework:

1. Assessing user vulnerability
2. Changing behaviour
3. Evaluating progress and tracking success

Step 1: Assess user risk and readiness

Every organisation is different, with unique risks and security priorities.

Ask yourself:

- Who is being targeted?
- With what types of attacks?
- How do you minimise risk if attackers get through?

By exploring these and other questions, you can determine where the vulnerabilities are. This exercise helps you focus on addressing the most urgent areas of exposure and potential compromise.

You should revisit this step regularly to reassess and recalibrate your approach.

How to measure user risk

Get specific, and make sure you pay attention to context by understanding your employee demographics and behaviour. It's critical to have contextualised metrics; different groups in the organisation behave differently.

A mistake organisations often make is measuring only what's easiest to measure. Reporting failed phishing attempts alone won't provide the whole picture of your security or employees' security awareness. Other measures organisations use to quantify security include mean time to detect (MTTD) threats and mean time to resolve (MTTR) threats. But some attacks take a long time to surface, so these measures are not always helpful either.

Meaningful metrics

Here are some of the best ways to assess user risk:

- Identify your most attacked users (including third parties, such as partners, vendors and contractors) by role and those who tend to click on links in emails. At Proofpoint, we call these users Very Attacked People™.
- Identify vulnerable users. Track user responses to phishing simulations that mirror current real-world threats. Note: Using a simulated phishing test is one way of identifying vulnerable users, but it shouldn't be the only metric. For example, users who perform poorly or don't participate in training exercises can also suggest areas of vulnerability. So those are key metrics to track, too.
- Find out what people do when no one is looking. Do they actively use password managers? Do they report phishing emails that come into the company? Do they share corporate information with noncorporate accounts?

Suggested activities

Here are some specific examples of things you can do to build a culture of security:

- **Monthly attack spotlights and training on trending threats.**
- **Weekly threat alerts with technical information to share with users via Slack or Teams channels and wiki pages.**
- **Rewarding accomplishments through motivational programmes that align with your company culture, such as leader boards or issuing prizes for reporting a phish that's real. This is especially important when getting started.**
- **Enlisting help from marketing and public relations staff to act as evangelists and help spread the word about security culture in a compelling and fun way (posters, emails, items in company or departmental newsletters, and internal blogs).**

Step 2: Change behaviour with threat-driven content and reinforced training

Building a security culture is an ongoing process, not a one-off event. Take a holistic approach.

That means reaching out to employees on a regular basis through multiple communication channels. These channels might include regular newsletters, internal blogs and updates on the latest threats and attack vectors.

You should also provide content that engages users and supports brand and culture needs. Tie training to the current threat landscape and make it more relevant to users. And create diverse types of content to train, engage and educate users: animated video, comedy or something more straightforward like quizzes. Offer a variety of content and personalise it. Everyone is different and reacts and learns differently.

Remember to continually reinforce the importance of security in a positive way. Put yourself in your employees' shoes and understand the demographics of the company. Employees have diverse interests.

Building a security culture hinges on users' sense of ownership. Create compelling, recognisable internal branding for your security programme.

Step 3: Evaluate and track your progress

Share metrics that show progress, continuous improvement and ROI. These quantifiable measures validate your investment, showing the value of a security culture to leadership and the organisation as a whole.

Never let a good crisis go to waste. After an attack, show how a stronger security culture reduced the amount of time, money and effort spent to resolve it—or helped the organisation avoid it altogether.

Here are specific metrics that can help you track your progress:

- Identify eight to 10 top-level security issues that you are focusing on and determine the risk they pose.
- Track time to update. Can you get everyone through a programme quickly? How do you accommodate and profile stragglers? (Why have they procrastinated? Is it because of a lack of motivation or something else?) How fast can you get employees to complete training?
- Highlight the activities used to actively promote the security culture. (Example: How often do managers update their team on the latest threats?)

What does success look like?

There are many ways to measure your organisation's level of security awareness so that you can evaluate how your security culture has changed user behaviour.

Click rates for your most vulnerable users

Vulnerable users are people who are more susceptible to phishing and other threats. By using phishing simulation templates tailored to various roles in your organisation, you can get an idea of who is avoiding malicious messages and who is clicking on them.

Resilience factor

Your "resilience factor" is measured by the phishing reporting rate for simulations divided by the phishing click. A goal to aim for is a 14x resilience factor, which translates to a:

- Reporting rate of 70% or higher for phishing simulations
- Click rate of under 5%
- Accuracy rate for reported email (are the emails users report actually malicious?)

Industry benchmarks

Executive dashboards show how you compare to your peers in key aspects of your security awareness programme. This insight enables you to pinpoint areas that could use improvement. For example, you can look at whether your users are reporting safe messages as malicious—and how that compares to other organisations.

Other metrics

Here are other people-driven security outcomes that you can factor in when assessing the success of your security culture:

- Successful phishing incidents
- The click rate for known malicious content
- Credential compromises
- Insider incidents
- Machine remediations due to ransomware

8 Keys to Building a Security Culture[13]

In one year, Jason Cox from Elevate Textiles, a global textile manufacturer, built a fully operational security culture.

Here are his "8 Simple Rules for Security Awareness":

1. Accept that people are the most targeted part of your business.
2. Involve senior leadership, as they can be instrumental in creating change and building stakeholder support.
3. Gather data to support your programme, using tools like cybersecurity assessments, surveys and logs for reported infections.
4. Deputise stakeholders and ensure they know the "why" behind the programme: Get manager buy-in for individual departments, as they know their people and what data to protect.
5. Saturate first, then build a routine. Pick a month to start (National Security Awareness Month in October can be opportune) and use it to immerse your users with education on key topics. After that, continue with regular touches and updates. Building a security culture is a continuous process.
6. Make it personal. How does information security affect employees at work and at home? Share personal stories. Make the programme fun and engaging.
7. Reward good behaviour with gift cards and other positive incentives.
8. Re-survey, report results, repeat. After a year, conduct a survey. Evaluate phishing tests again. Tally the number of security tickets. And stay in touch with senior leaders who must answer to risk and liability and need to know the benefits of the programme.

[13] Adapted from a presentation at the 2021 Proofpoint Wisdom conference (https://www.proofpoint.com/us/wisdom-2021-demand-content-library).

Conclusion

Creating a strong, continuous security culture benefits the entire cross-section of your users—from the C-suite to the security team to managers and end users.

But there's no one-size-fits-all template for a security culture. Every organisation has a different personality and unique needs. Some of these differences are driven by the business. Others by the industry. And every culture is driven by a whole host of internal and external factors.

By building an enduring programme that gets buy-in at all levels, security awareness becomes ingrained in your organisation's core values. A true security culture is not just about a one-time security training session. It's a mindset that informs day-to-day business and personal activities.

To learn more about how Proofpoint can help you build a security culture tailored to your unique business culture, visit: https://www.proofpoint.com/uk/products/security-awareness-training.

LEARN MORE

For more information, 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 75 percent of the Fortune 100, 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.