sosafe

Behavioral Security

How to Boost Security Awareness with the Help of Behavioral Metrics

Table of Contents

01 Introduction

The power of behavioral science in cyber security

There is no way of denying it: Information security is one of the most pressing challenges organizations face these days. Not only have cyberattacks become more common – they are also more sophisticated than ever, as many criminals have understood the power of social engineering – making their attacks tricky to detect and even trickier to avert.

As such, the social engineering tactics used by attackers to emotionally manipulate their victims are strongly connected to human behavioral patterns. And so must the respective security measures designed to protect organizations from these attacks. The dynamic changes in the threat landscape have urged many security professionals to rethink their protection strategies and move from mere technical measures toward a more holistic, human-centered approach to cyber security. As part of this paradigm shift, behavioral change has become a key term – if not the key term – that organizations now focus on to build a strong security culture. A culture engaging employees to reflect on their behavior and build secure routines gives cybercriminals less of a chance to do harm.

Understanding the behavior of both attackers and users, and how successful certain measures are in changing user behavior, therefore gives organizations the opportunity to anticipate attacks and neutralize them early on. Clear and meaningful behavioral metrics not only help decision makers understand how employees react to different types of threats, but also to determine whether a specific type of training works for them. Additionally, it gives them the opportunity to constantly adapt their awareness initiatives based on these results. For example, if a specific team shows lower phishing reporting rates than others, some e-learning nudges might do the trick in getting these employees to better understand how to detect and report suspicious emails. Ultimately, behavioral metrics powerfully illustrate the cultural impact the programs have on an organization's overall security. Such tangible metrics are invaluable tools in discussions with all stakeholders involved, from C-level executives to employees.

That brings up two questions

Which metrics should organizations focus on when evaluating the impact their initiatives have on their security culture?

And which methods from behavioral science boost said impact on security awareness?

To answer them, we need to first explore the interconnectedness of behavioral science and cyber security, and then dive deeper into the dimensions shaping a holistic security culture as well as the metrics revealing the effectiveness of the different security measures.

02 What makes organizations move toward measuring behavioral change in cyber security

To those within cyber security, it is common knowledge by now: Technology alone is not enough anymore to protect organizations from the cybercriminals' increasingly sophisticated attacks and their latest scam tactics. Social engineering has become the go-to for attackers as they have realized the success rates for attacks on the human factor are shockingly – for them, positively – high. **In fact, more than 82 percent of all data breaches involve a human element** according to Verizon's latest Data Breach Investigations Report.[1] IBM similarly lists credential fraud and phishing – both strongly connected to the human factor – as the top two attack vectors. [2]

Companies are paying a high price for criminals' innovation

This shift in the threat landscape has already led to costly consequences for organizations all over the world, amongst those big names like Twilio, Cisco, and Uber. All three companies just recently experienced the imminent danger of social engineering themselves.

In Twilio's case, hackers got access to more than 120 customer accounts after employees had fallen prey to "a sophisticated social engineering attack designed to steal employee credentials" [3], as the company phrased it. The criminals used personalized phishing messages via text messaging ("smishing") to trick employees into disclosing sensitive information.

Threat intelligence provider Cisco Talos similarly informed the public that almost 3GB of data were stolen in a breach linked to the Yanluowang ransomware gang.[4] The criminals had managed to gain control of an employee's personal Google account in which the employee had stored sensitive log-in credentials. They then tricked employees into accepting MFA processes via voice phishing ("vishing") to ultimately get into the company's systems.

1 Verizon (2022). Data Breach Investigations Report.
2 IBM (2022). Cost of a Data Breach Report.
3 Twilio (2022). Incident Report: Employee and Customer Account Compromise.
4 Cisco Talos (2022). Cisco Talos shares insights related to recent cyber attack on Cisco.

Perhaps the most striking of all, global transport services giant Uber faced a social engineering attack supposedly initiated by an 18-year-old hacker in September 2022.[5] By surpassing a vulnerable MFA process and using a man-in-the-middle tactic, the attacker made an administrative user unknowingly pass on credentials – giving the intruder access to Uber's internal environment such as data storages and communication platforms.

Remote work and technological progress increase the risk of cyberattacks

However, cybercriminals' innovativeness and novel tactics are just one side of the coin. Many other factors are additionally driving the current development toward human-centered cybercrime tactics. The past two years have given rise to a multitude of remote working models, including new processes and collaboration tools. And with these tools come new possibilities for attack. Apart from equipping cybercriminals with new entry points into the company systems, the introduction of tools and processes also often leads to transitional periods in which employees are more insecure and therefore prone to deception. At the same time, technological progress takes its toll on information security more generally. Artificial intelligence (AI) is not to be underestimated in this regard. Techniques like voice cloning, by which the voice of a person is artificially cloned and used in phishing attacks, are becoming easier to implement. AI-as-a-service tools might soon make these new attack tactics accessible even for lay people and will give current attack tactics such as spear phishing a whole new dynamic.

The key question is: How do we protect ourselves from these threats?

Although security awareness has long played a role in security strategies for companies of all sizes and industries, it is now undergoing a paradigm shift. Old training models that rely on ticking off regulatory requirements and static content libraries are not effective in protecting organizations from the latest threats that come with the professionalized cybercrime industry. What it takes is a mature security culture – and a holistic approach to security awareness. Instead of focusing on compliance alone, measures should effectively foster secure habits in employees so that they know how to act securely in everyday work life. And by adopting principles from behavioral science into security awareness programs, companies can finally move from one-time measures towards continuous security culture management that provides effective protection against social engineering.

[5] Ars Technica (2022). Uber was breached to its core, purportedly by an 18-year-old. Here's what's known.

The perks of measuring behavioral change

Getting to this point, however, also involves drawing on relevant metrics that illustrate the development of their security culture and employees' change in behavior. These behavioral metrics are powerful tools in the day-to-day of CISOs and other security professionals.

Adding them to their strategies and reporting has several advantages:

They help to understand the typical behavioral patterns of employees, for example, in case of an attack. How do they react? Which attack tactics are they most vulnerable to? What helps them learn – and what disturbs their learning process?

They give decision makers the chance to counteract those vulnerabilities and improve their security measures accordingly. Do employees need more motivators to get their training done? Which topics should they dive into in more detail again?

They serve as tangible arguments in discussions with stakeholders from C-level to employees to showcase how secure habits can positively influence the overall security of a company – and may even be tied to financial success metrics of the company. How has the awareness program helped foster secure behavior and minimize the risk of a costly attack, for instance?

Defining the metrics relevant to your organization

The question of which exact behavioral metrics organizations should look at has no easy or universal answer. For every company, professionals might want to have a closer look at KPIs that are specific to their needs and contextual situation, such as their industry type. These behavioral metrics can move well beyond attack reporting rates or training completion rates. Besides behavioral data collected during awareness training, this might include online behavior such as using a password manager, the acceptance of internal policies, or downloading apps only after approval by IT. Ultimately, sophisticated behavioral metrics will help estimate the complex KPI that is cyber risk – and give organizations the chance to get the ball rolling on proactive defense mechanisms where needed.

INFOBOX

Combining traditional awareness metrics with next-gen behavioral metrics

As part of the paradigm shift, organizations are well advised to move away from only using "traditional" performance-based metrics (such as phishing click rates) and, instead, to also include more holistic behavioral metrics (like phishing reporting rates). Together they can readily illustrate the impact awareness measures have on secure behaviors that are anchored in the organizational culture.

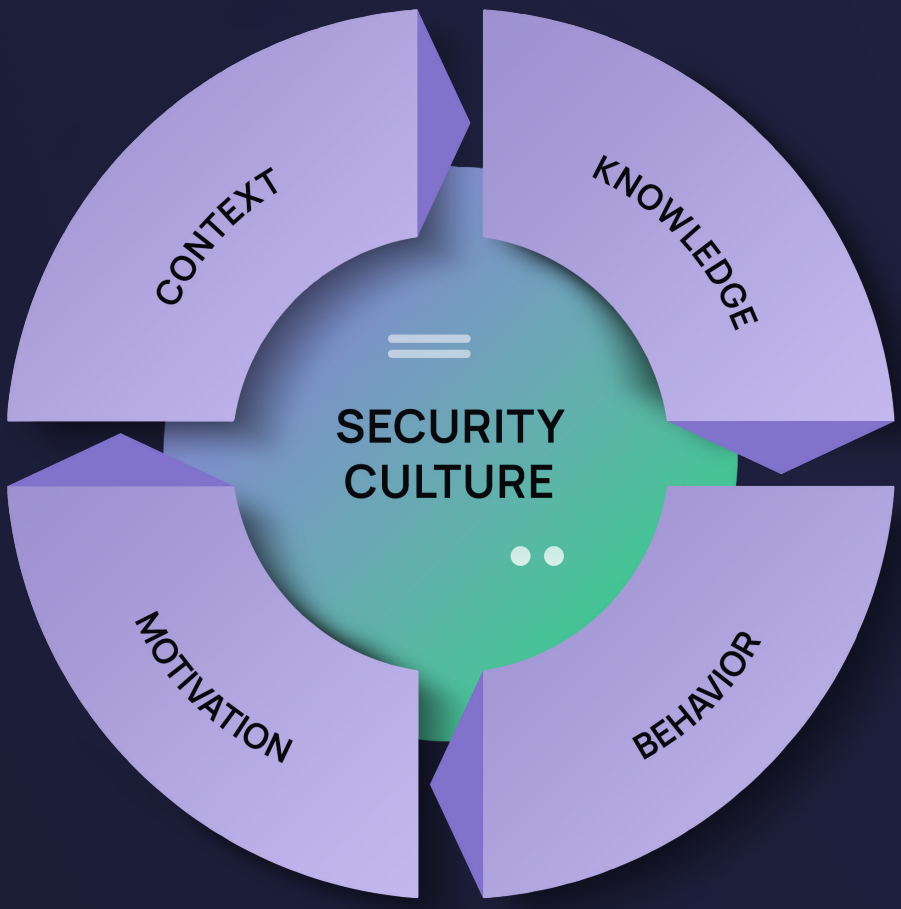
The following table gives examples of different types of these metrics:

Traditional awareness metrics	Next-generation behavioral metrics
Click rates in phishing simulations	Phishing reporting rates using integrated reporting tools
Open rates in phishing simulations	Interaction rates with simulated phishing mails and pages
Completion rate of a password security course	Daily or weekly usage rates of a password manager
Completion rate of a data confidentiality course	Number of data assets properly tagged with their confidentiality status on company intranet
Viewing rate of a video about shadow IT	Number of software approval requests to IT

As the previous sections have illustrated already, including behavioral science in security is not a straightforward process nor do the same guidelines apply to every organization. So, let's have a look at the dimensions that constitute a mature security culture first – and at some of the behavioral metrics and methods organizations can use to strengthen theirs.

03 The Behavioral Security Model:

Building a human-centric security culture



Cyber threats pose an ever-expanding challenge as they continue to evolve. And there is no doubt now that the common thread connecting the majority of cyberattacks is the human factor. Despite all technical precautions, organizations aren't safe without recognizing their employees as part of the solution to the trillion-dollar problem that is cybercrime. Access to sustainable and effective training is key to securing organizations' human layer.

The "Behavioral Security Model" emphasizes the core components of such a human-centric approach to security, each contributing to the overarching goal of building a protective security culture. Instead of viewing them as discrete components, we can consider them to be driving a behavioral flywheel. The strength of each component simultaneously boosts digital self-defense, as they all reinforce one another. Gathering the right metrics to understand the maturity of your security culture in each of these dimensions will help identify security risks and proactively address them.

3.1 Knowledge: Delivering insights and best practices that stick

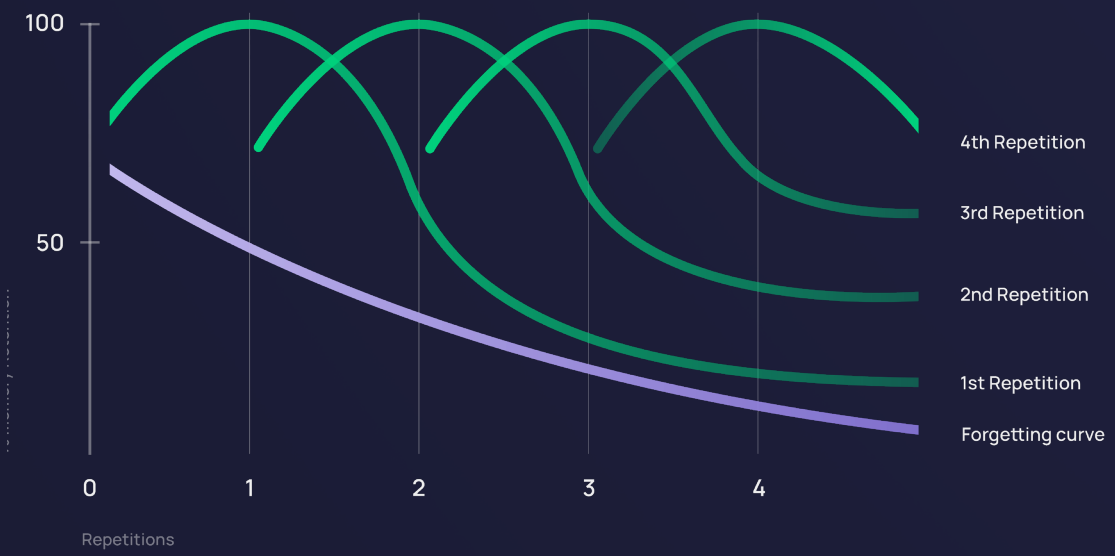
Lack of human-centered training can unintentionally encourage carelessness towards cyber security. When employees aren't engaged, they don't find a compelling reason to be proactive and reactive to cyberattacks, risking the security of both them as individuals and the company. It's a no-win situation. Security programs should be designed to make employees understand the role they play in recognizing and reverting potential attacks. In order to show certain safe behaviors, employees need to be equipped with knowledge about security best practices first.

The biggest motivation to increase their knowledge should be this: Hackers never stop learning. This already underscores the importance of including ongoing education within organizations. In the past, knowledge was often conveyed linearly and in high doses. We know all too well, though, that long workshops and monotonous learning sessions are not just outdated, but do not achieve what training promises: Knowledge that actually sticks to memory. That is because knowledge retention will naturally exponentially decline, which poses significant challenges when it comes to learning and development.

According to Ebbinghaus' Forgetting Curve [6], within a training context, learners can forget 90 percent of what they learn within the initial 7 days. The rate of information drop increases when users break their learning patterns and frequency. But there are ways to retain training efforts that enhance information recall. Spaced training consistently delivered via different channels lets users repeat what they have learned. In combination with interactive and motivating elements like quizzes, this makes for an effective strategy to combat the forgetting curve.

SPACED TRAINING

Example of a learning path encouraging knowledge repetition



6 Growth Engineering (2020). What is the forgetting curve?

> "Nudging continuously increases engagement by 30 percent and even up to 90 percent in the introductory phase"

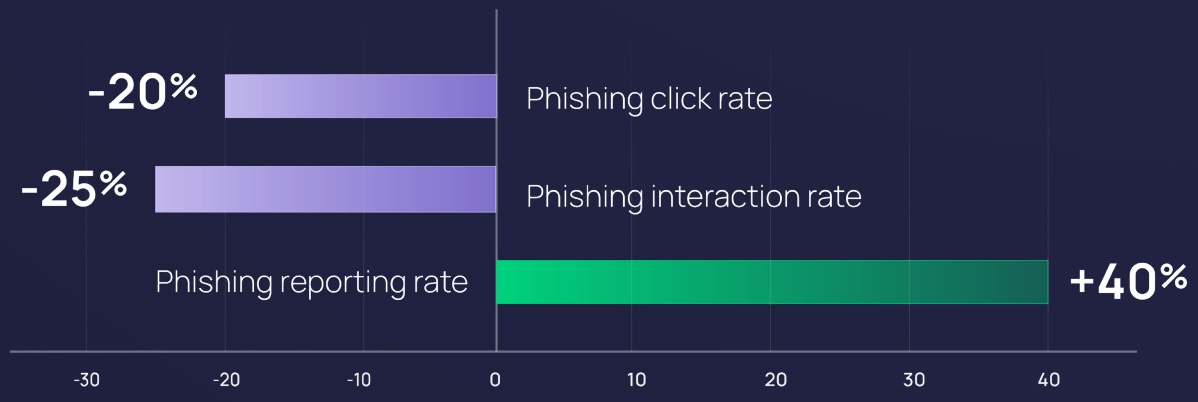
One method to account for a more sustainable learning experience via spaced training are nudges. As mentioned in our latest Human Risk Review: "Nudging continuously increases engagement by 30 percent and even up to 90 percent in the introductory phase." [7] Nudging in the form of regular, automated system emails, for example, nurtures interactions with users and keeps awareness in front of mind. Nudges can take the form of encouragements, reminders, and progress updates, among others, to ensure users are consistent with their awareness training.

Knowledge that is positively reinforced through methods like spaced learning and nudging is key to nurturing a strong security culture as data impressively illustrates. For example, those who complete learning modules on cyber security and data protection are better at identifying and deterring malicious emails like phishing attempts. **These employees are also 40 percent more likely to report phishing attempts compared to those who have a lower module completion rate as data from the SoSafe platform shows.**

All in all, employees who have a solid understanding and knowledge of how to ensure digital self-defense will help their organizations reduce the risk of incidents. A sound training program with continuous, contextual knowledge delivery can efficiently support this.

PRODUCT USAGE

Results from users with high module completion rates



Example behavioral metrics in the knowledge dimension

- → E-learning completion rates
- → Impact of nudging on engagement rates
- → Impact of e-learning completion on phishing reporting rates

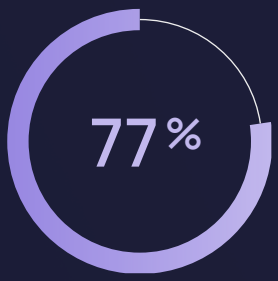
[7] SoSafe (2022). Human Risk Review 2022.

3.2 Context: Learning that aligns with individual risk factors

The level of complexity of cyber security training is affected by another essential factor that opposes the one-size-fits all approach: Context. To standardize the security starting points of all employees would be overlooking the inherent singularities that exist within the organization. For example, executive managers or employees with a company cell phone are exposed to greater danger than internship roles.

Therefore, different hierarchies within your organization are likely to be targeted differently by cybercriminals. This isn't to suggest that all employees aren't at risk – which they are – but ensuring that all threat levels receive relevant attention under a uniform response plan. Organizations therefore need to have a clear understanding of the roles and responsibilities their employees carry along with which kinds of risks they can expect or be exposed to. Since this will differ for all employees, the training should be customized accordingly.

Having personalized paths will make the learning experience tangible and relevant, and minimize cyber risks effectively. According to research conducted by Towards Maturity, 77 percent of learners seek content that is relevant to their work. [8] This behavior-based approach focuses on the employees, addresses their unique challenges, and delivers content specific to their roles, profiles, and awareness levels.



of learners seek content that is relevant to their work

[8] Towards Maturity (2017). Modern learning content for modern workers.

The industry a company operates in also has an influence on the risk. Healthcare, banking, and the public sector are some of the most targeted. Sharing specific internal policies within security training platforms, therefore, can be vital to boosting employee awareness. The more contextual the knowledge is, the better the information recall can be for employees.

There is another dimension of context in this approach: Organizations should not only provide personalized learning options, but also create a context that encourages safe behavior. Incorporating components and tools within the existing infrastructure can enable employees to take an active stand. This is easier with a data-driven awareness platform that integrates specific features to make it easier to spot and report suspicious digital activity. For example, employees who have access to the SoSafe Phishing Report Button show a 30 percent lower interaction rate with phishing emails, as compared to those that do not have this functionality. That means attacks are less likely to lead to success with this contextual feature. **There are other demonstrable benefits to having a reporting button feature:**

IMPACT OF PHISHING REPORT BUTTON

E-learning adoption rate

Module completion rate

Therefore, in order to help employees nurture and polish the right skills and knowledge needed to be able to make informed decisions, organizations should, firstly, personalize the learning experience and make it relevant to the learners and, secondly, provide them with the right contextual tools to act securely. Each employee will then be able to see for themselves the impact they have on the security wellbeing of their organization and continue their training with a reinforced sense of commitment.

Example behavioral metrics in the context dimension

- → Engagement rates with/without personalized learning
- → Phishing reporting rates with integrated reporting tool
- → Impact of reporting tool usage on e-learning completion

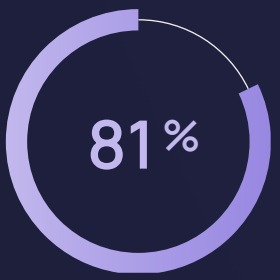
3.3 Motivation: Engaging employees for improved learning outcomes

A robust security culture thrives when employees are enabled, engaged, and educated. Along with having access to learning tools and technologies, it is important to nurture a receptive environment that involves the entire organization, irrespective of roles and responsibilities. The commitment to security should trickle from the top down to be embraced across teams, which is why leadership must make it their mission to inspire a holistic culture instead of creating siloed security. Among the internal and external factors influencing a mature security culture, motivation stands out.

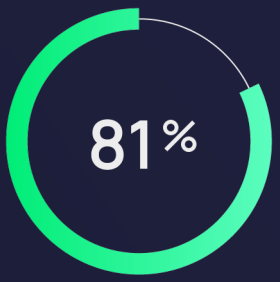
Motivation can be argued to be qualitative, undefined by digits. But while its multidimensional nature cannot be measured explicitly, it can be assessed through various correlated factors like progress, effort, and achievement. Delivered via gamification, for example, it makes a positive impact on direct engagement. Compared to traditional classroom-style sessions, engaging modules with gamified e-learning have been shown to catalyze interest, integration, and participation that ultimately fuel motivation for employees. According to a survey conducted by Talent LMS, more than 80 percent of the respondents feel gamification fuels creativity, helps them learn better and feel more connected, and offers a sense of purpose overall.

As progress is monitored and knowledge is acquired, motivation is both a booster and a by-product. There is a reciprocal relationship between motivation and learning, as it mobilizes users to act.

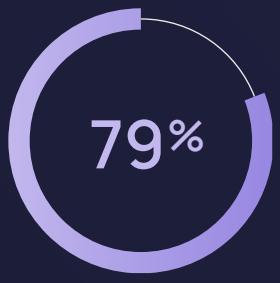
Gamification provides a **greater sense of creativity, choice, freedom** and/or **responsibility**



Gamification makes me feel **more socially connected** and provides a **sense of belonging**



Gamification **helps me learn and develop** personally and professionally



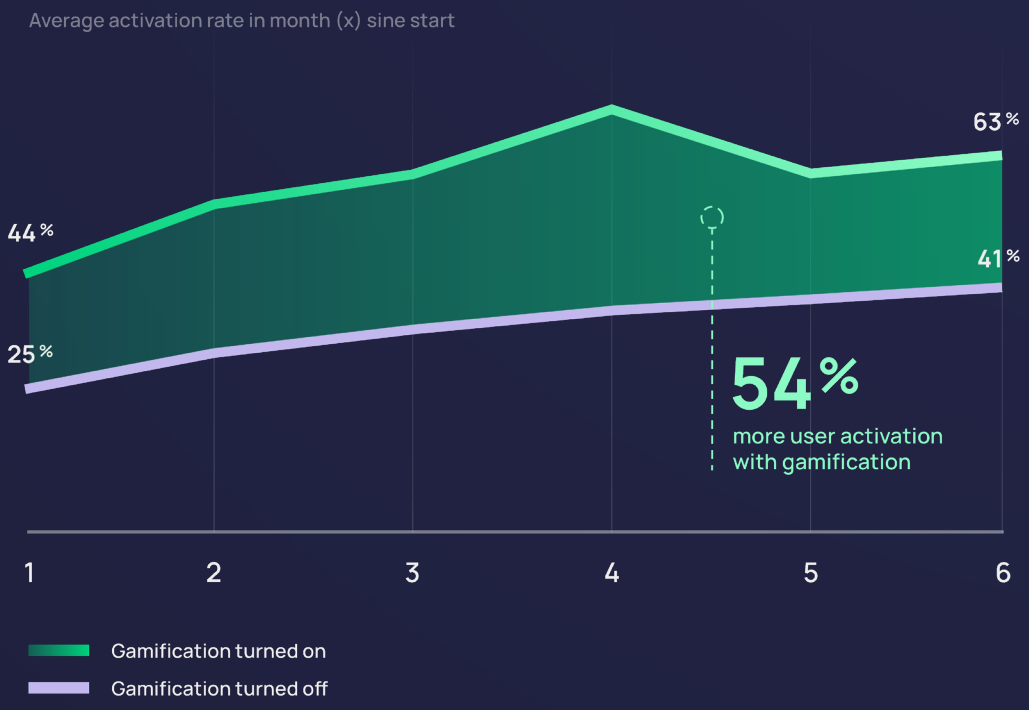
Gamification provides a **greater sense of meaning and purpose** in my workplace

Source:
TalentLMS (2018). The 2018 Gamification At Work Survey.

Data-driven platforms like SoSafe that are designed with behavioral science have been shown to make a lasting impact on motivation, within the complex subject area that is cyber security. With compelling narratives, levelled challenges, and well-earned incentives, deep gamification has been shown to increase activation by more than 50 percent in users. If employees find security topics boring and complex, they won't have intrinsic motivation to learn more about them. And in stressful everyday work environments, it is likely that they feel they have little time for these topics. Integrating typical elements from computer games into the learning process proves successful in increasing the fun factor and therefore motivates continuous learning.

PRODUCT USAGE

Gamification boosts user engagement, increases security awareness, and is fun



An immersive learning experience enables employees to receive the instant feedback they need to make their corrective actions become their reflective actions. And they are motivated by being rewarded along their journey.

Example behavioral metrics in the motivation dimension

- → E-learning activation rates
- → Impact of gamification on e-learning completion

3.4 Behavior: Making secure habits second nature

The pivotal element in every strong security culture is behavior – as frequently measured in the metrics shown in the previous chapters. Locking your screen when you are away from your desk, scanning your emails for suspicious activities, and letting IT know about risks and incidents early on – it all comes down to secure employee routines and habits to safeguard your organization. Measuring how awareness training changes these behaviors can be beneficial in adapting the program accordingly, thereby effectively minimizing cyber risks.

As should have become clear already, fostering these daily digital (workplace) habits is strongly dependent on the other three dimensions: Only if employees are knowledgeable about information security, equipped with the right contextual setting, and intrinsically motivated, will they continuously show secure behavior. Whether it be the impact of spaced learning on knowledge retention, how motivation boosts engagement rates, or how creating an empowering learning context for employees increases phishing reporting rates – all these metrics show how security culture is a holistic approach. Focusing on one of the dimensions exclusively or checking off compliance requirements with a single on-site presentation on security, aren't successful anymore in the dynamic threat landscape that we find ourselves in today.

Instead, decision makers should use insights from all dimensions of the Behavioral Security Model to adapt their awareness program so safe habits become second nature for employees.

Example behavioral metrics in the behavior dimension

- → Phishing reporting rates via reporting tool
- → Interaction rates with phishing emails and pages
- → Daily or weekly usage rates of a password manager
- → Differentiated click rates depending on psychological tactics used
- → Time to reporting

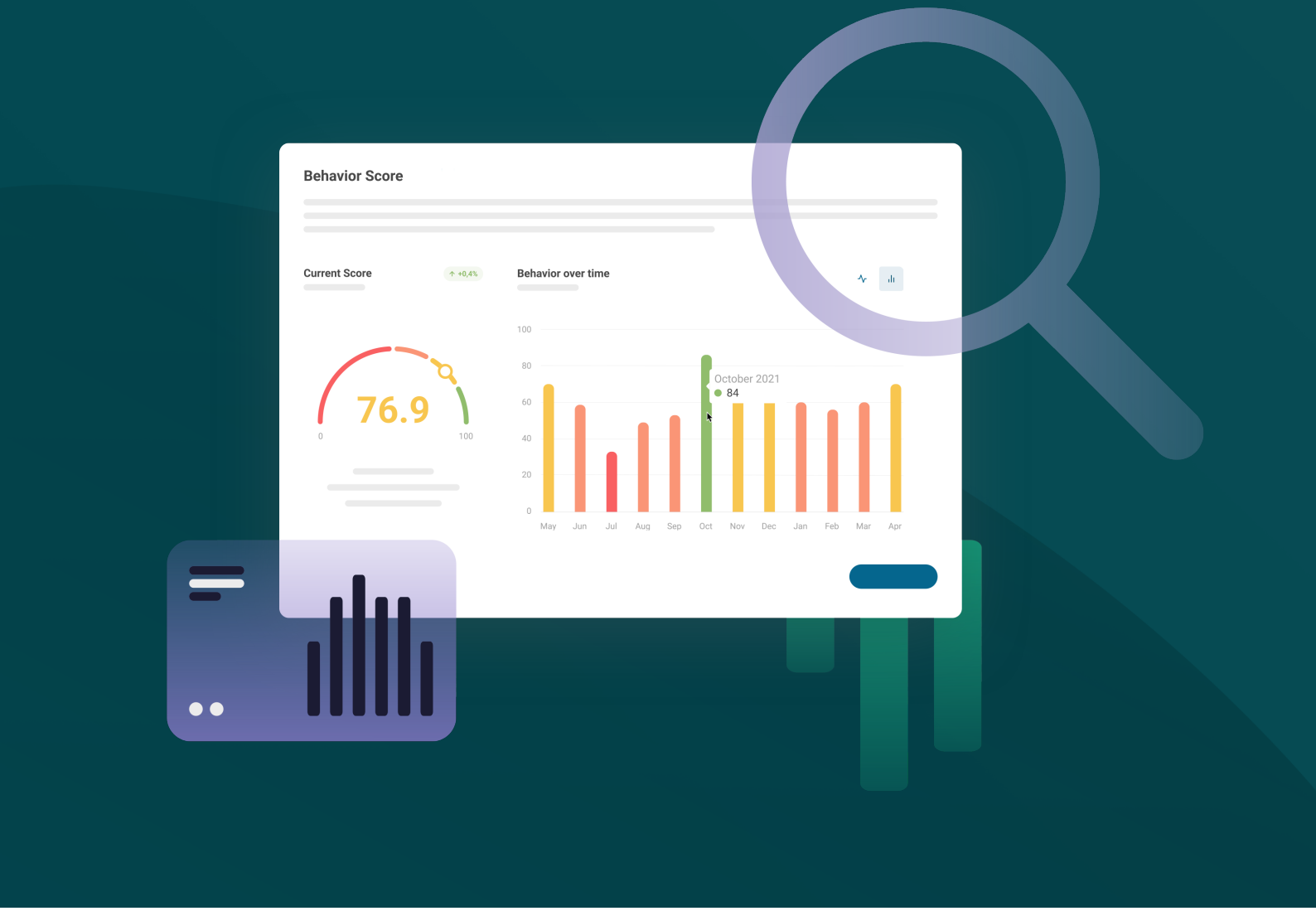
04 Why measuring security behavior pays off

The strength of an organization's security culture is heavily driven by a combination of factors that influence secure habits. A strategy that reinforces the security posture should meet the employees at their level of exposure and expertise. The main dimensions of our Behavioral Security Model exhibit how each factor – knowledge, context, motivation, behavior – continuously influences the others to form the foundation of modern security awareness – one that extends beyond any checklist.

Apart from traditional methods of training, empowering employees with an immersive educational experience is not only engaging but effective. This is further proven when their behavior is measured. Tracking the right metrics within a security training program that aligns with your organizational goals can help identify where stronger habits are developed and where weaker ones need to be strengthened. Instead of turning a blind eye towards training, organizations need to adopt a proactive approach to security before expecting their employees to be able to do the same.

There shouldn't be assumptions on how much employees know and how they will behave when targeted with a cyber threat. Instead, implementing a security awareness program that trains, teaches, and transforms carelessness into secure habits is the approach to adopt. Measure these changes to understand which specific aspects your organization needs to catch up on. And throughout this process, employees are expanding their know-how and being rewarded for doing something that is securing a lot more than data: learning.

Next-generation awareness solutions like SoSafe offer behavioral metrics that give insight into the success of the training as well as point out any existing vulnerabilities that need immediate attention. More than that, recommendations pertaining to security risks provide you with guidance on spotting, understanding, and mitigating potential threats.



What is your Behavior Score[BETA]?

The Behavior Score is a phishing performance indicator designed to answer three key questions often asked by information security officers:

1. How likely is my organization to fall victim to a phishing or social engineering attack?
2. How can I easily summarize employee performance to senior stakeholders, without needing to go into too much detail?
3. What can I do to increase our score and exceed industry benchmarks?

How It Works

Currently in Beta, the Behavior Score scores an organization based on three different phishing simulation metrics: click rate, interaction rate, and reporting rate (for users of our Phishing Report Button). The score is displayed as a number on a scale of 0 -100. If sufficient data is available, you will also see an industry benchmark - the average result of the top 20 best performing companies in your industry.

Interaction rate

Engagements with simulated fraudulent websites, for example inputting login data

Click rate

Clicks on a link in a phishing simulation mail

Reporting Rate

Phishing simulations reported via the Phishing Report Button

Your Score and What it Means Today

Building
<58

Your employees engage in phishing simulations at a higher rate than the industry average, leaving your organization vulnerable to threats. Consider doubling down on email security awareness to quickly and efficiently close this gap.

Solid
58-68

Your outcome is likely to be comparable to the industry average, and you have established a solid foundation. Familiarize employees with advanced attacks (such as customized spear-phishing) to strengthen your human firewall.

Strong
69-77

Your organization's recognition and avoidance of phishing attacks is above average. If you haven't already, it's time to work on establishing a strong reporting culture in addition to your overall security culture.

Leading
77+

Congratulations – not many organizations make it to this level. Your score suggests that your company has a strong security culture. You have a challenging but exciting task ahead of you: keep engagement and behavior at the highest level.

Scale your security culture with ease!

With its awareness platform, SoSafe empowers organizations to strengthen their security culture and mitigate human risk. The platform delivers engaging learning experiences and smart attack simulations that help employees become active defenders against online threats – all powered by behavioral science to make the learning journey both fun and effective. Comprehensive analytics measure the behavioral change impact and tell organizations exactly where vulnerabilities lie so they can proactively respond to cyberthreats. The SoSafe platform is easy to deploy and scale, effortlessly fostering secure habits in every employee.

Engaging Micro-Learning

A behavioral science-based learning platform that employees love:

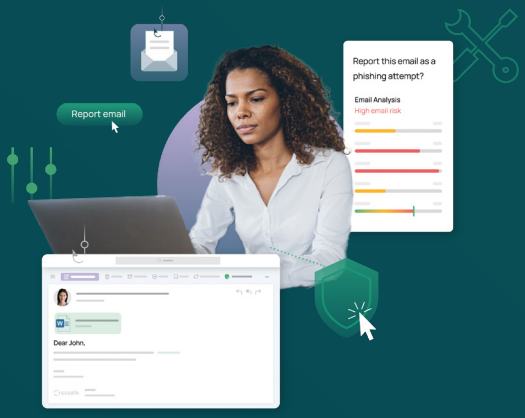
Strengthen your resilience to cyberthreats and fulfill compliance obligations with dynamic and impactful learning experiences across channels to build long-lasting, secure habits with ease.

- → Story-driven, gamified learning content designed to engage and stick
- → Curated and guided content library readily scalable for growth
- → Low-effort customization and content management to fit every organization

Smart Attack Simulations

User-centric phishing simulations that foster secure habits:

Help employees learn to spot cyberattacks using automated spear phishing simulations that create situational and steady awareness moments – to effectively reduce risk and crucial threat detection time.



- → Personalized and realistic cyberattack simulations
- → Context-based learning walkthroughs to reinforce secure employee behavior
- → One-click reporting of threats via integrated Phishing Report Button

Strategic Risk Monitoring

Comprehensive human risk dashboard that helps to proactively respond to vulnerabilities:

Use advanced analytics to get an overview of your organization's risk, manage and interpret the behavioral change impact of your awareness program, and make data-informed decisions.

- → Tracking of contextual data including technical and psychological KPIs
- → Industry benchmarking and actionable insights on key areas of improvement
- → Built for ISO/IEC-27001 requirements, and based on a privacy-by-design approach

SoSafe GmbH
Lichtstrasse 25a
50825 Cologne, Germany

info@sosafe.de
www.sosafe-awareness.com
+49 221 65083800