Debunking the “stupid user” myth in security

Exploring the influence of employees’ perceptions and emotions on security behaviors

nudge

Executive Summary

Humans have long been considered the weakest link in cybersecurity. Unlike the security pillars of technology and process, people are unpredictable: fallible, limited, and error prone. As such, the cybersecurity industry goes to great lengths to protect organizations against the inevitable threat of the human element.

Despite this effort, people still routinely fail to comply with security controls at work. Why? Are people really just “stupid users,” or is something else at play?

Our research found that human emotion is a strong predictor of security behavior. Participants in our study were less likely to comply with a security control if they perceived the experience to be negative or unreasonable.

In fact:

- **74%** felt negatively about SaaS access being blocked; **67%** said they would look for a workaround.
- Security nudges were perceived as positive up to **9X** more often, and **78%** of participants said they would comply with a nudge.

To date, the industry hasn’t widely considered how people *feel* about their experiences with cybersecurity, and how those experiences impact security outcomes. Yet, our research suggests that by understanding the psychology of this “human element,” we can find new ways to encourage better security behaviors and create stronger security systems.

We hope you enjoy this report.

The Nudge Security team

Table of contents

Introduction

We wanted to study how employees' attitudes and emotions influence their security behaviors. So, we turned to Nudge Security advisor Dr. Aaron C. Kay, PhD, J Rex Fuqua Professor of Management and Professor of Psychology & Neuroscience at Duke University, to discuss the role that human psychology plays in workplace cybersecurity. As an academic researcher, Kay studies how different motivational forces affect people's opinions and behaviors within organizational settings. For example, his past research revealed that people who are passionate about their jobs are more susceptible to being exploited by their employers, which he coined as the passion tax.

Drawing on Kay's wealth of expertise, we hypothesize that failures to comply with security controls they experience or interact with in the workplace (which we refer to as "security interventions") cannot be chalked up entirely to user error, incompetence, or indifference. We felt there was something else at play. We suspected that people's likelihood to comply with a security control is motivated, in part, by their opinions, emotions, and experience when facing a security intervention. These types of psychological factors are woefully overlooked and understudied by the cybersecurity industry.

Through our conversations with Dr. Kay, we surfaced the following questions, which became the basis for our research:

- Why do people routinely fail to comply with security controls?
- Do perception and emotion play a role in security decision-making?
- Are people less likely to comply with a security control if they think it's unreasonable or frustrating?
- Inversely, are people more likely to comply with a security control if they find it to be reasonable or a positive experience?
- Could a more reasonable, positive experience actually improve compliance with a security control and thus, better security outcomes?

Research Overview

With assistance from Dr. Kay and Dr. Matthew Stanley, Postdoctoral Research Associate, Fuqua School of Business, Duke University, we designed a research experiment to investigate how people's attitudes and emotions influence their security behaviors at work.

Our research took 900 participants through a common scenario: needing to access a SaaS application for work. Participants were randomly assigned to one of three security interventions, described below. Participants were asked to rate how reasonable they found the intervention, how positively or negatively they felt about it, and how likely they were to comply or not comply with it.

The status quo: conventional security interventions

We identified two conventional security controls that represent the types of security interventions employees most commonly experience in the workplace. The first is the use of network-based security technologies (firewalls, gateways) that limit and monitor employees' access to data, IT systems, and even parts of the internet. In our research experiment, this preventative control was represented in our "blocking intervention" scenario. It was designed to prevent participants from accessing a SaaS application needed to complete a work task.

The second conventional control we identified is the use of security education, training, and awareness (SETA) programs that aim to improve employees' security behaviors. In addition to periodically scheduled events, security training is often used as a way to reinforce and remind employees of desired security behaviors after some policy infraction. In our research experiment, this corrective control was represented as our "punitive intervention" scenario. It was designed to retroactively terminate participants' access to a SaaS application needed to complete a work task and require participants to undergo additional security training.

The security nudge: a friendlier security intervention

To develop our “friendly” security intervention, we reviewed the core tenets of nudge theory, a theory popularized by behavioral economists Richard Thaler and David Sunstein in their 2008 book, Nudge. In it, they describe a nudge as:

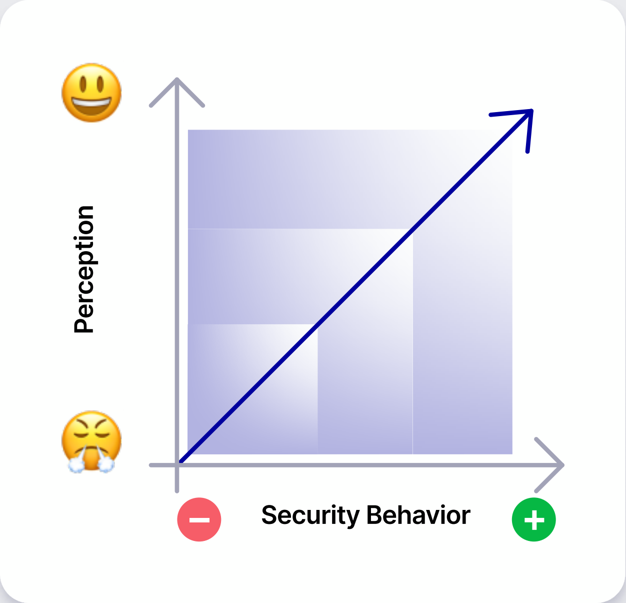
> “Any aspect of the choice architecture that alters people’s behavior in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid. Nudges are not mandates. Putting the fruit at eye level counts as a nudge. Banning junk food does not.”

We developed the concept of a “security nudge”—a highly contextual and timely security intervention that aims to guide employees toward desired security behaviors without blocking them (“forbidding any options”) or reprimanding them (“changing their economic incentives”). In our research experiment, our security nudge served as our “nudging intervention” scenario. It was designed to initiate a security conversation with participants as soon as they started the process of accessing a new SaaS application needed to complete a work task.

Key Findings

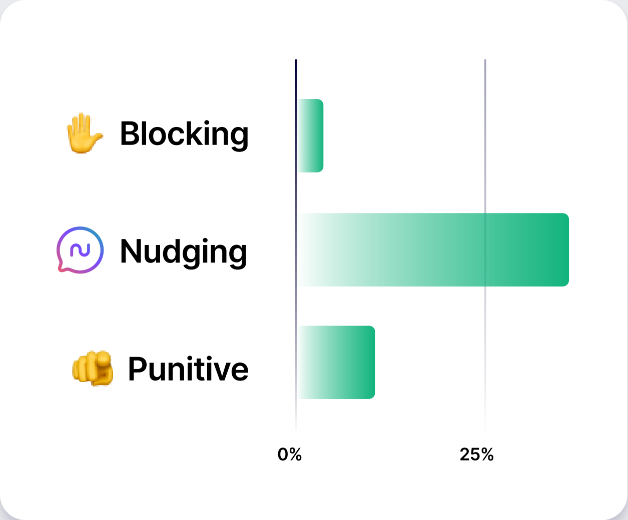
Attitudes and emotions are strong predictors of behavior—even when it comes to cybersecurity.

Across all security interventions examined, the results show two consistent trends. First, the more reasonable participants found the intervention, the more likely they were to comply with it. Second, the more negative participants felt about an intervention, the less likely they were to comply with it. These findings suggest that people’s attitudes and feelings are good indicators of their likelihood to comply with security controls. Despite being largely overlooked and understudied to date, they should be considered as critical design factors by the cybersecurity industry.



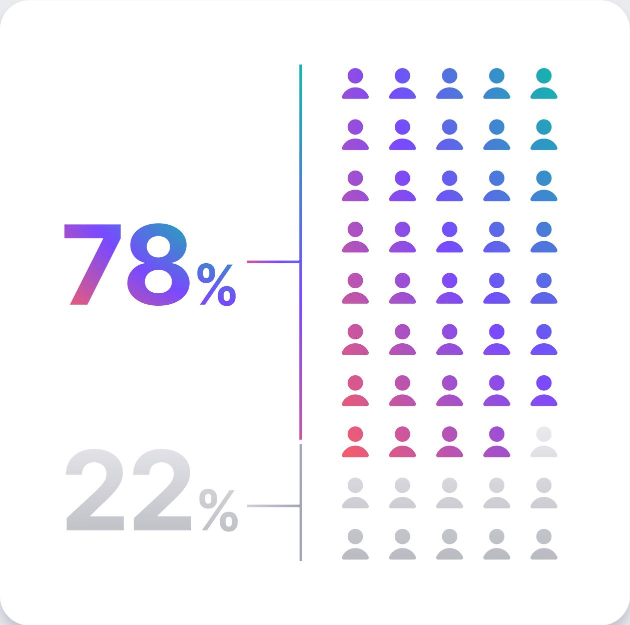
Overall, participants were most positive about security nudges as a security intervention.

Participants found security nudges to be more reasonable than conventional security interventions. Similarly, participants in the nudging scenarios were significantly less likely to react with negative emotions compared to the conventional security interventions. Compared to the nudging intervention, participants in the blocking scenarios were **3 times more likely** to respond with negative emotions. Given the positive relationships we saw across attitudes, emotion, and behaviors, we expected that security nudges would also drive a high rate of compliance—and they did.



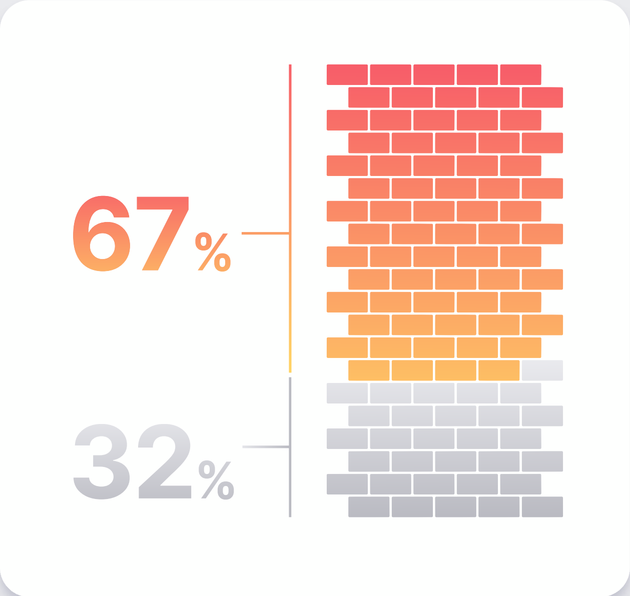
Participants were highly likely to comply with security nudges.

Compliance with security nudges was very high. In fact, **78%** of participants in the nudging scenario said they would be likely to respond to the security nudge. For comparison, only **32%** of participants in the blocking scenario said they would be likely to comply with the intervention.



And yes, when you block access to applications, people look for workarounds.

It might come as no surprise that **67%** of participants in the blocking scenario said they would look for a workaround to access the application that had been blocked. This suggests that security interventions that attempt to block or limit access to applications that employees need to complete their work may ultimately lead to counterproductive security outcomes.



Further Discussion

A research experiment for modern work

Our research experiment centered around an increasingly common workplace scenario: an employee needs to access a new SaaS application in order to complete a work task. We deliberately chose this scenario because it reflects the new realities of modern work and the inherent cybersecurity risks these new realities evoke.

Modern workers now consider themselves to be technology experts, after a global pandemic increased everyone's reliance on web-based technologies for work and personal use. Today, employees at mid-sized enterprises are adopting new SaaS tools at the rate of one new SaaS account every 2 minutes, and one new SaaS provider every 5 days. Workers also want autonomy over their technology choices. According to a recent survey, nearly half of digital workers say they're likely to leave their current job if they're unhappy with workplace tech.

These new realities of modern work run against the grain of conventional enterprise IT, cybersecurity, and GRC paradigms, which rely on small groups of experts having complete visibility and control over the organization's IT assets. Hybrid work and IT consumerization have made it increasingly difficult for governance teams to maintain centralized visibility and control, especially using network- and endpoint-centric security technologies built for a bygone era of office buildings, workstations, and intranets.

In the delta between modern work and conventional governance, threats emerge. Threat actors have set their sights on insecure shadow SaaS accounts, complex digital supply chains, and easy-to-compromise user credentials. Security teams must act to secure these environments, but they often find themselves outpaced and outnumbered by the rate of SaaS adoption across the organization. As our research shows, security teams can no longer rely on "locking and blocking" approaches to stem the tide of adoption as employees find more ways to optimize their work. (Arguably, these approaches were never really effective anyway.)

Security and governance teams need a new approach—one that empowers modern employees to leverage the cloud and SaaS technologies they need to move the business forward while also encouraging those same employees to adopt and consume that technology in highly secure ways. Our research points to the promising potential for security nudges to make this a reality.

Next steps: give us a nudge.

We plan to continue this exploration of positive security behavior change. Nudge Security was founded to transform the human element of cybersecurity for modern work. We envision a future where every person is empowered to take control of their identity, security, and privacy online. We recognize that our best opportunity to begin to work towards this vision is by influencing positive security behavior change in the workplace.

Nudge Security launched a technology platform to help cybersecurity and IT governance teams drive such behavior change by making it easy and automated to engage employees and nudge them towards better security decisions and behaviors as they adopt and use cloud and SaaS technologies. In doing so, Nudge Security allows organizations to unlock technology choices for employees while also giving governance teams the oversight they need to manage cyber risks in today's SaaS-powered world.

Jump to About Nudge Security →

Methodology

Study design

Nudge Security developed this research. Dr. Matthew Stanley, Postdoctoral Research Associate, Fuqua School of Business, Duke University, and Dr. Aaron C. Kay, PhD, J Rex Fuqua Professor of Management and Professor of Psychology & Neuroscience at Duke University, assisted in designing and developing the materials and experiment.

Our study focused on people's attitudes, emotions, and behaviors in response to various security interventions (described below). We used a between-subjects experimental design, meaning that participants were randomly assigned to one of three experimental conditions. In each condition, we asked questions about participants' opinions, feelings, and likelihood to comply or not comply with the intervention. We conducted this study in August 2022 through an online survey.

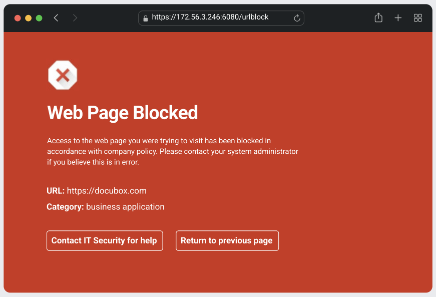
To begin, we gave all participants the same hypothetical prompt. Then, participants were randomly assigned to one of three conditions below, each condition representing a different type of security intervention. We asked all participants questions about their attitudes, emotions, and behaviors related to the security intervention they had observed.

Step 1 “Imagine yourself in the following scenario at work: you need to access a file from a third-party partner outside your organization in order to complete an important task.

The partner sends you a secure email link to access the file from a reputable online file sharing application, DocuBox. You click on the link in the email to access the file.”

Step 2 “When you click on the link in the email, it takes you to this web page:”

Blocking Condition


https://172.56.3.246:6080/urlblock

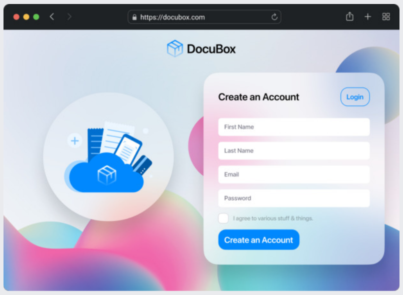
Web Page Blocked

Access to the web page you were trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

URL: https://docubox.com
Category: business application

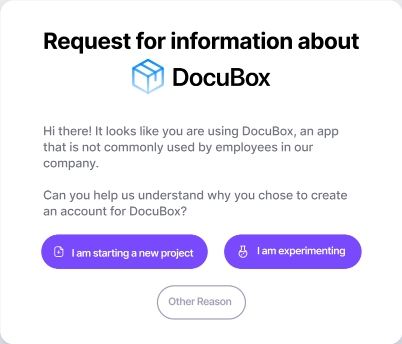
Contact IT Security for help
Return to previous page

Nudging Condition



You sign up for a DocuBox account with your corporate email address.

You then receive the following email message from your organization’s IT security department:

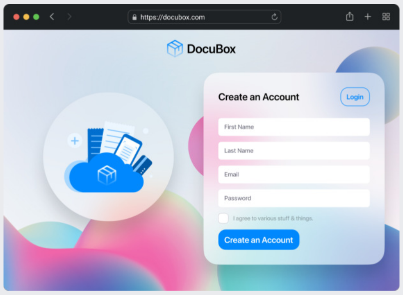


Request for information about DocuBox

Hi there! It looks like you are using DocuBox, an app that is not commonly used by employees in our company.

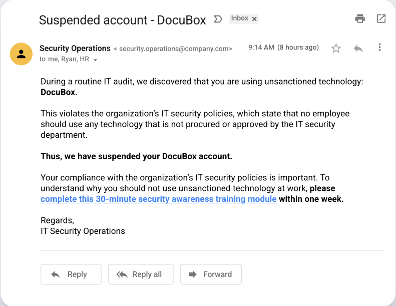
Can you help us understand why you chose to create an account for DocuBox?

Punitive Condition



You sign up for a DocuBox account with your corporate email address.

You then receive the following email message from your organization’s IT security department, and your direct supervisor is copied on the email:



Suspended account - DocuBox

Security Operations < security.operations@company.com> 9:14 AM (8 hours ago)
to me, Ryan, HR

During a routine IT audit, we discovered that you are using unsanctioned technology: **DocuBox**.

This violates the organization’s IT security policies, which state that no employee should use any technology that is not procured or approved by the IT security department.

Thus, we have suspended your DocuBox account.

Your compliance with the organization’s IT security policies is important. To understand why you should not use unsanctioned technology at work, **please** complete this 30-minute security awareness training module **within one week.**

Regards,
IT Security Operations

Variables & measurements

In order to measure the differences in participants' reactions to the three experimental conditions we used the following measurements.

Attitudes

To measure participants’ attitudes about the security interventions, we asked how reasonable they found the messages in the security interventions to be. To determine reasonableness, we asked participants to what extent they disagreed or agreed with the security intervention being (1) sensible, (2) helpful, and (3) easy to comply with. We used an interval 5-point Likert-type scale, where:

1 = strongly disagree
2 = somewhat disagree
3 = neutral
4 = somewhat agree
5 = strongly agree

Our reasonableness variable was a composite (average score) of these three items.

Emotions

To measure participants’ feelings about the security interventions, we asked how positively or negatively they would feel about the messages in the security interventions. Again, we used a 5-point Likert-type scale to measure participants’ emotional valence, where:

1 = very negative
2 = somewhat negative
3 = neutral
4 = somewhat positive
5 = very positive

Behaviors

To measure participants' behaviors, we asked how likely they would be to (1) comply with the message in the security intervention and (2) not comply with the message in the security intervention. We used a 5-point Likert-type scale to measure participants' likelihood to comply and not comply, where:

1 = very unlikely
2 = somewhat unlikely
3 = neutral
4 = somewhat likely
5 = very likely

For each condition, we adjusted the language slightly to describe each act of compliance and non-compliance in a way that was most logical within each condition. For example, in the blocking condition as a measure of non-compliance, we asked participants, "How likely would you be to look for an alternative way to access DocuBox?" In the punitive condition as a measure of compliance, we asked participants, "How likely would you be to complete the security awareness training module within one week?"

Limitations

Across all conditions, we used the same variables and measures for reasonableness and emotional valence. However, because we adjusted the language for each behavior-related question, we were not able to compare and contrast the average measures of compliance and non-compliance across the conditions as we did for the first two variables.

Study sample

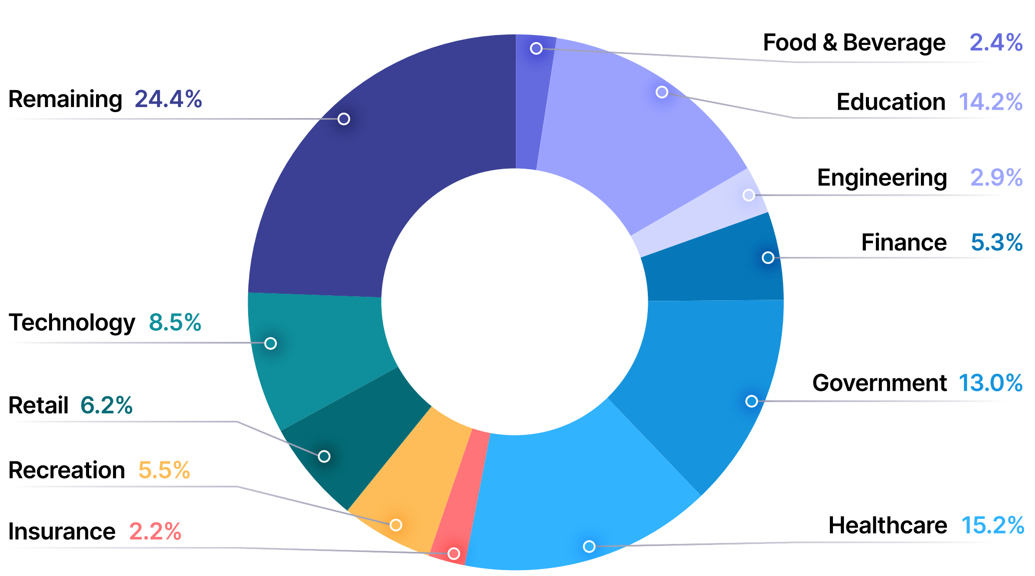
For this study, we recruited participants in the United States and the United Kingdom who met all of the following criteria:

- have been employed for at least the past 24 months
- are currently employed full time
- use software at work at least once a week
- are employed at organizations of at least 1000 employees

We wanted to recruit participants who were more likely to have had some workplace exposure to IT security programming. As a proxy, we assumed that organizations of at least 1000 employees are more likely to have some degree of IT security programming, policies, and / or personnel as compared to organizations of a smaller size.

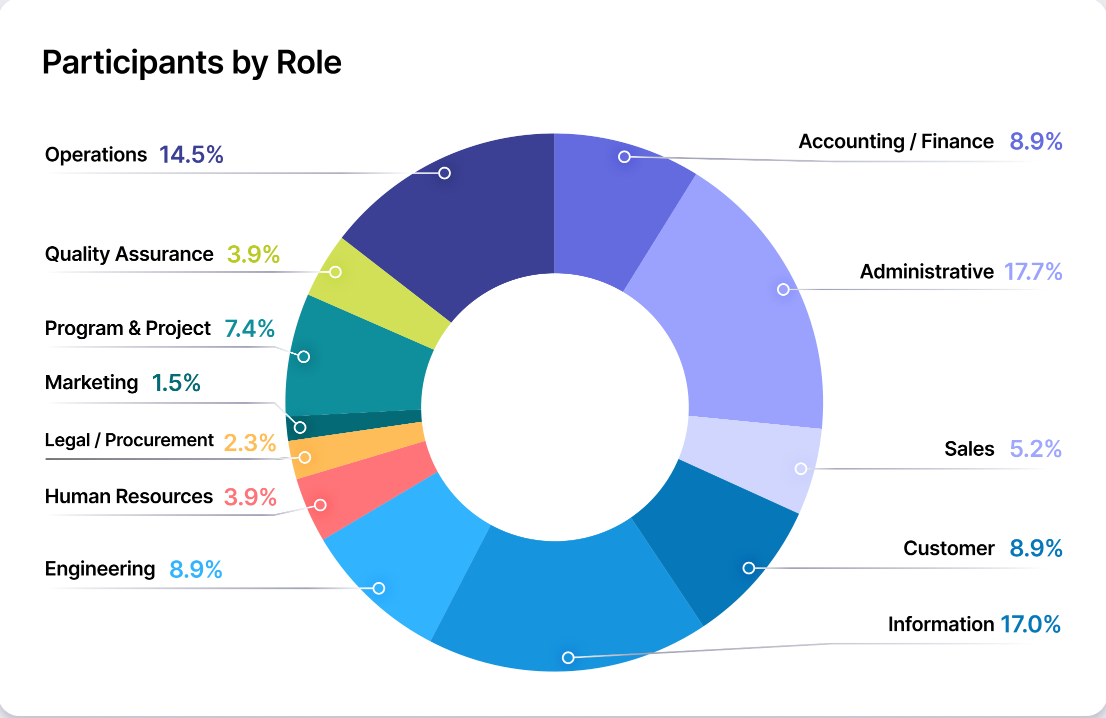
We recruited 901 participants for this study (mean age = 39 years, age range = [19 years, 70 years]). The following graphs provide more information about participants and their work situations, broken out by cohort.

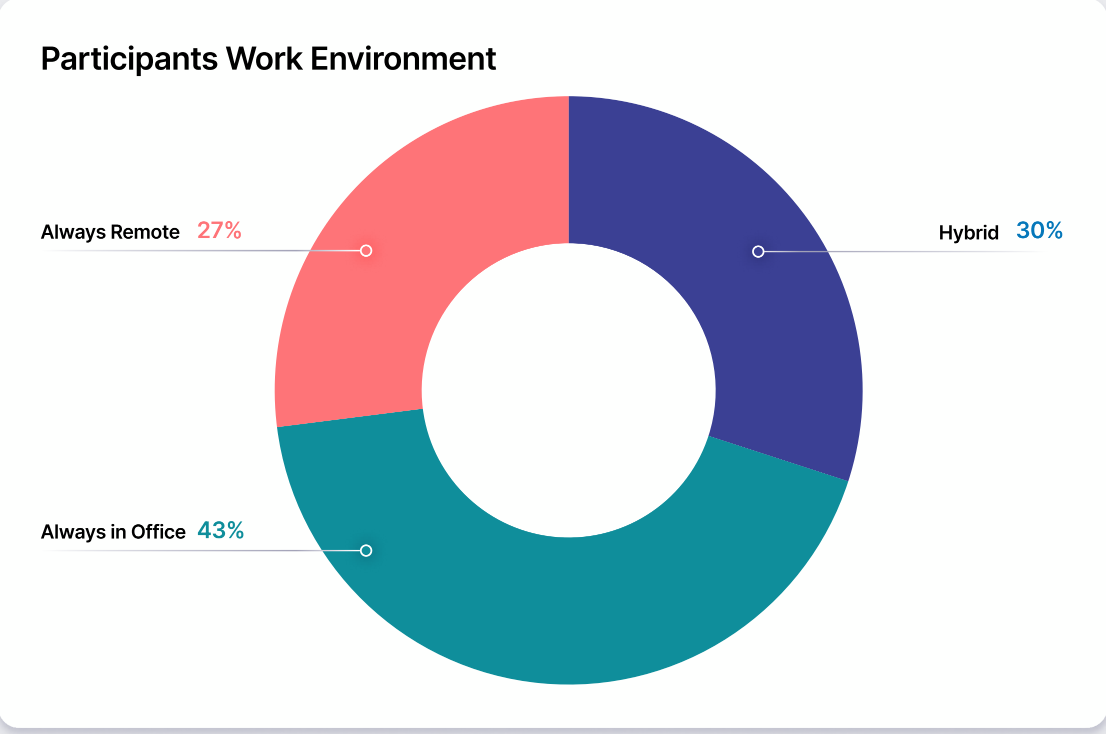
Participants by Industry



Study sample

This donut chart shows the breakdown of experiment participants by reported roles / job function.





Results

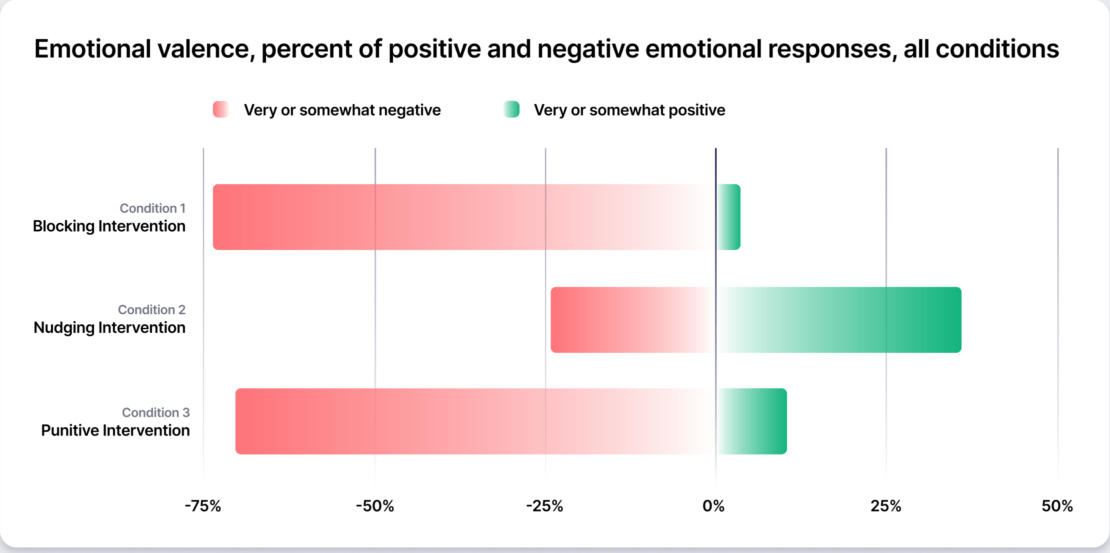
Emotions

Participants felt significantly more positive about security nudges than conventional security interventions.

Talk about warm fuzzies and cold pricklies: participants were nearly **3 times** more likely to feel negative about conventional security interventions than security nudges.

- Participants presented with the nudging intervention (n = 298) reacted negatively only **24.2%** of the time.

- Participants who were presented with more conventional security interventions reacted negatively **72.1%** of the time.
  - In the blocking intervention (n = 301) **73.8%** had a negative reaction.
  - In the punitive intervention (n = 301) **70.4%** had a negative reaction.



Survey Question

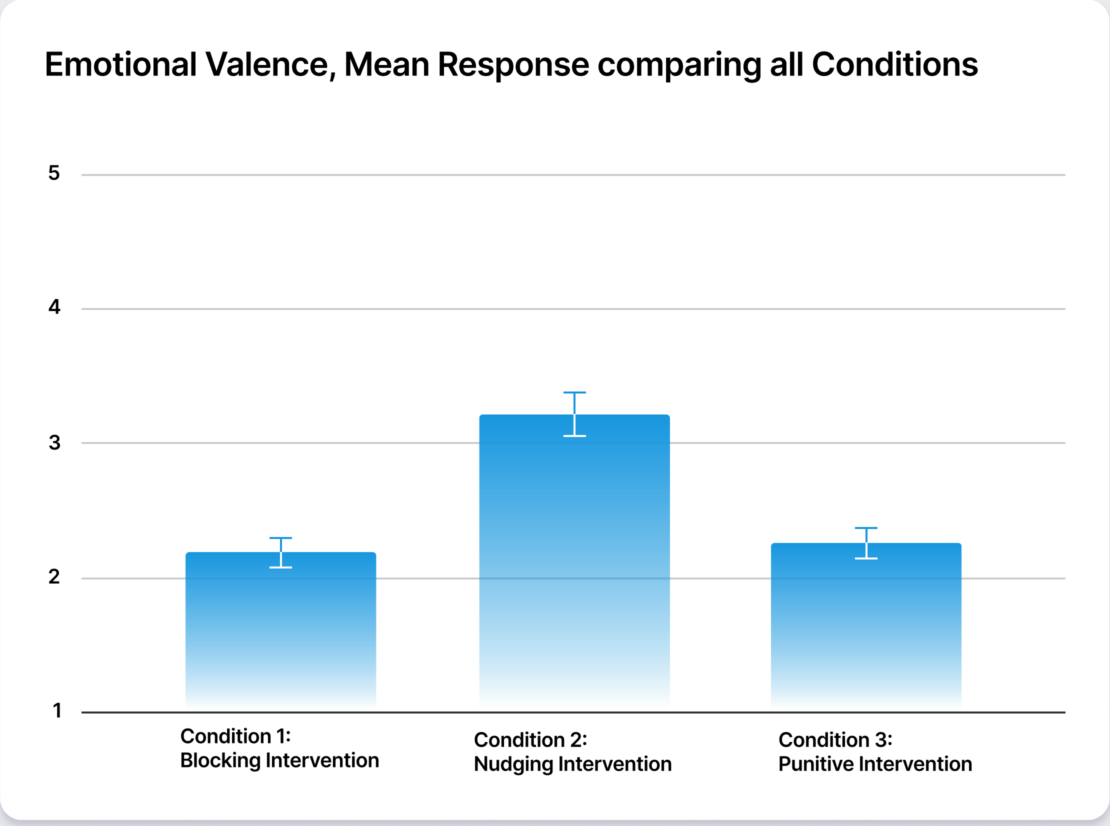
Having seen the message above (intervention), how would you feel?

1 = very negative
2 = somewhat negative
3 = neutral
4 = somewhat positive
5 = very positive

Key Takeaway

Similar to attitudes, employees' feelings about the security interventions were strong predictors of their likelihood to comply. Security leaders should not assume that employees will treat security controls as bad-tasting medicine, hold their noses, and swallow. Emotion is a strong motivational factor of behavior, and security leaders should work with their colleagues to develop security interventions that the workforce will embrace, not just tolerate.

This is an increasingly important discussion as organizations continue to face the threat of widespread attrition and employee disengagement. Boards and executive teams are scrutinizing every aspect of the employee experience, looking for opportunities to reduce friction and frustration. CISOs have an opportunity to contribute to organizational goals of employee engagement and satisfaction by creating a more positive security experience.



Figure

Overall, participants felt more positive about the nudge intervention than the blocking intervention (Mean difference = 1.03, p < .001, 95% CI [.89, 1.17]) and the punitive intervention (Mean difference .96, p < .001, 95% CI [.82, 1.09]).

Nudge Mean = 3.22; SE = .06
Block Mean = 2.19; SE = .04
Punitive Mean = 2.26; SE = .05

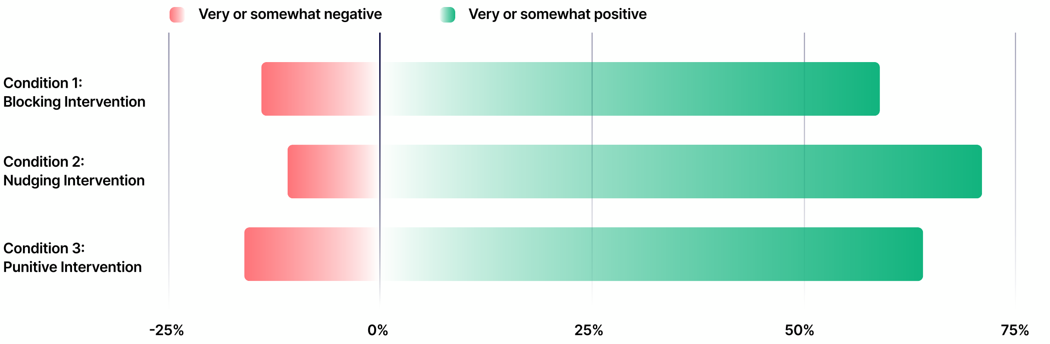
Attitudes

Participants found security nudges to be the most reasonable security intervention.

Overall, participants in the nudging condition found it to be much more reasonable (sensible, helpful, and easy to comply with) than in the blocking and the punitive conditions. 212 participants found security nudges to be reasonable compared to 183 participants in the blocking condition (-29 fewer than in the nudging condition) and 193 participants in the punitive condition (19 fewer than in the nudging condition).

- **71%** of participants in the nudging condition (n=298) strongly or somewhat agreed that the security nudge message was reasonable, whereas only **11%** strongly or somewhat disagreed.
- In the blocking condition, (n=301) **59%** strongly or somewhat agreed that it was reasonable, while **14%** strongly or somewhat disagreed.
- In the punitive condition (n=301), **64%** strongly or somewhat agreed that it was reasonable, while **16%** strongly or somewhat disagreed.

Perceived reasonableness, percent of responses in agreement and disagreement, all conditions

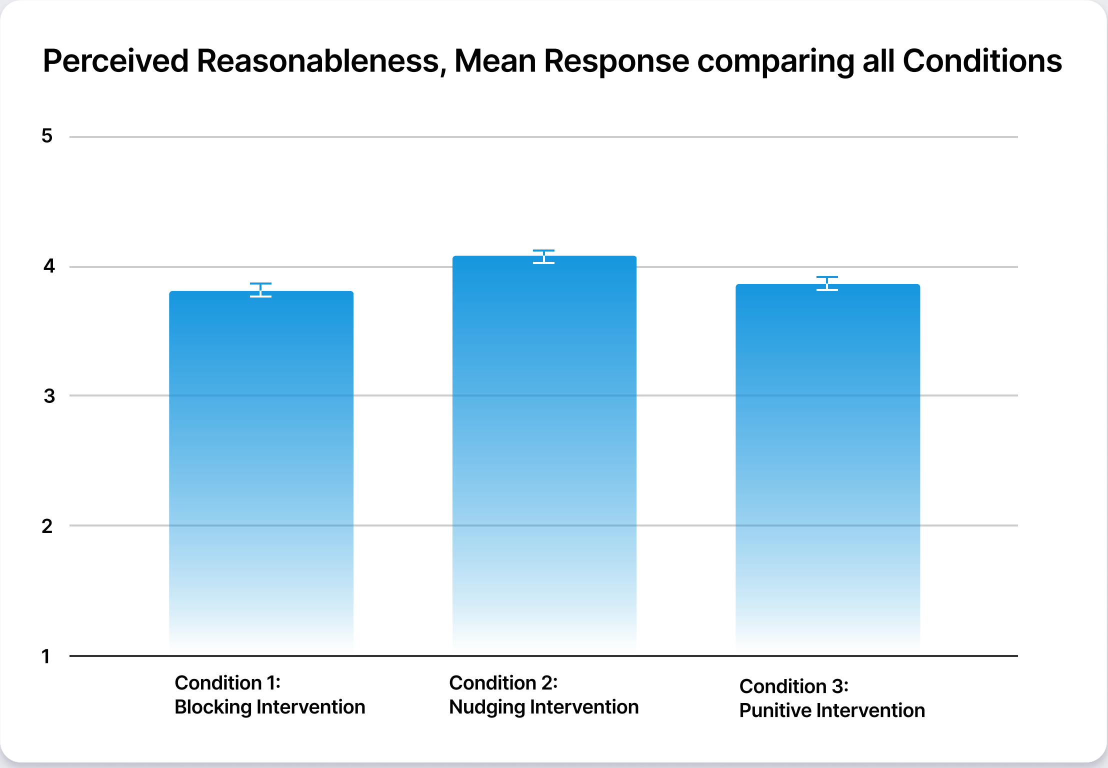


Figure

This chart shows the percent of participants who strongly or somewhat disagree with the reasonableness of the condition in contrast to those who strongly or somewhat agree with the reasonableness of the intervention. Reasonableness scores that were neutral (between 3.0 and 4.0) are not shown.

Key Takeaway

As we discuss later in the report, employees' attitudes about the security interventions were strongly linked to their likelihood to comply. This may seem intuitive, but it's rarely put into practice. Security leaders seeking to improve compliance with their security policies should consider asking the general workforce what they think about proposed policies, perhaps through an employee survey. This would be a radical departure from the ways in which IT security policies are commonly enacted within organizations today.



Figure

This chart compares the mean score of perceived reasonableness across all conditions. Overall, participants reported that the nudging intervention was much more reasonable than blocking security intervention (mean difference = .26, $p < .001$, 95% CI [.12, .41]) and the punitive intervention (mean difference = .22, $p = .003$, 95% CI [.07, .36]).

Nudge Mean = 4.08; SE = .05
Block Mean = 3.82; SE = .05
Punitive Mean = 3.87; SE = .06

Survey Question

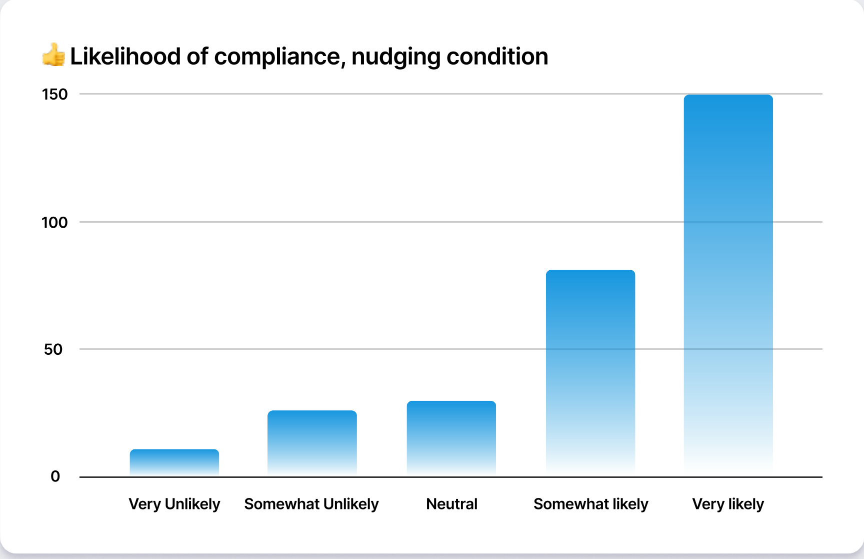
Having seen the message above (block, nudge, or punitive condition), to what extent do you agree or disagree with the statements below? Please indicate your level of agreement using the scale where 1 = strongly disagree, 2 = somewhat disagree, 3 = neutral, 4 = somewhat agree, and 5 = strongly agree.

This message is sensible.
This message is helpful.
This message is easy to comply with.

Behaviors

Participants were very likely to comply with security nudges.

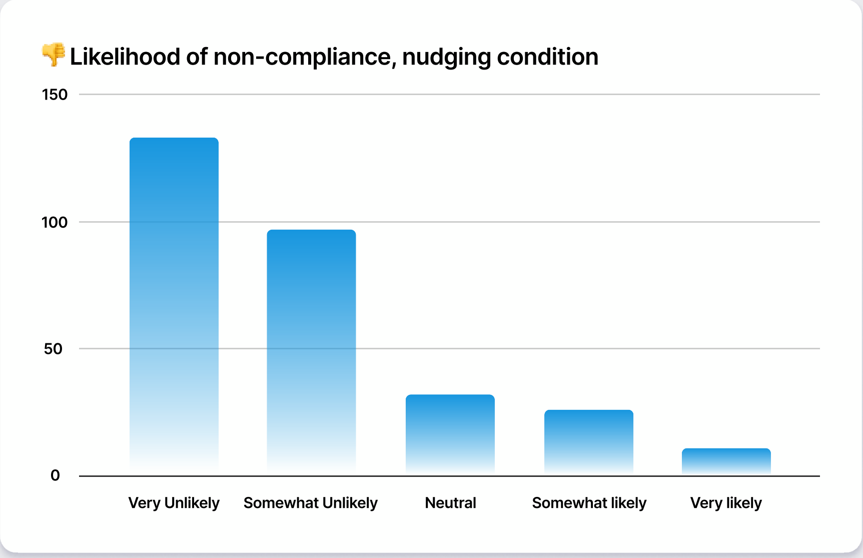
Not only did participants feel positive about security nudges, but also they were happy to engage with them. In fact, **78%** of participants in the nudging condition reported that they were somewhat or very likely to respond with the security nudge, whereas only **12%** said they were somewhat or very unlikely to respond to the security nudge. When the question was asked in reverse (How likely would you be to ignore the security nudge?), the results were nearly identical.



Survey Question

How likely would you be to respond to the message from IT with the information requested? (Comply)

1 = very unlikely
2 = somewhat unlikely
3 = neutral
4 = somewhat likely
5 = very likely



Survey Question

How likely would you be to ignore the message from IT? (Non-comply)

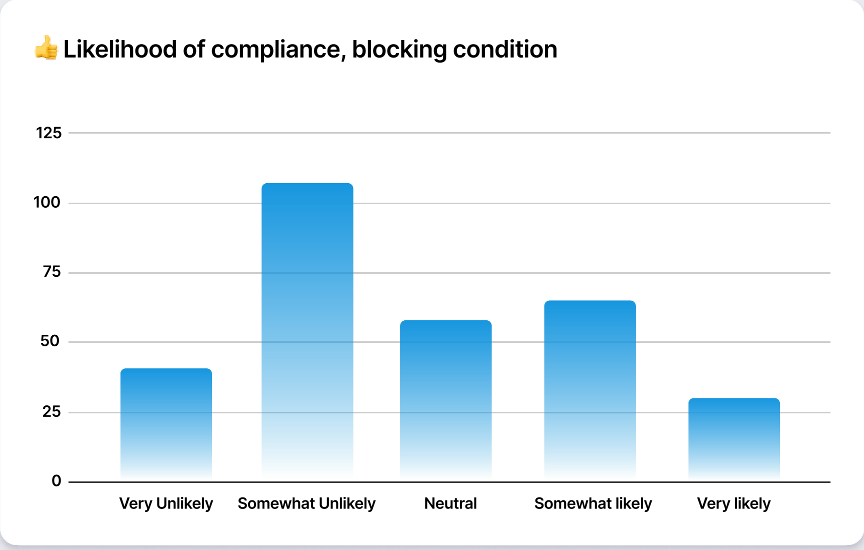
1 = very unlikely
2 = somewhat unlikely
3 = neutral
4 = somewhat likely
5 = very likely

Research notes

In the nudging condition, participants report that they would be unlikely to ignore the message, on average (M = 1.95, p < .001) and that they would be very likely to reply to the message with the information requested, on average (M = 4.12, p < .001).

When blocked, 67% of participants would likely seek a workaround.

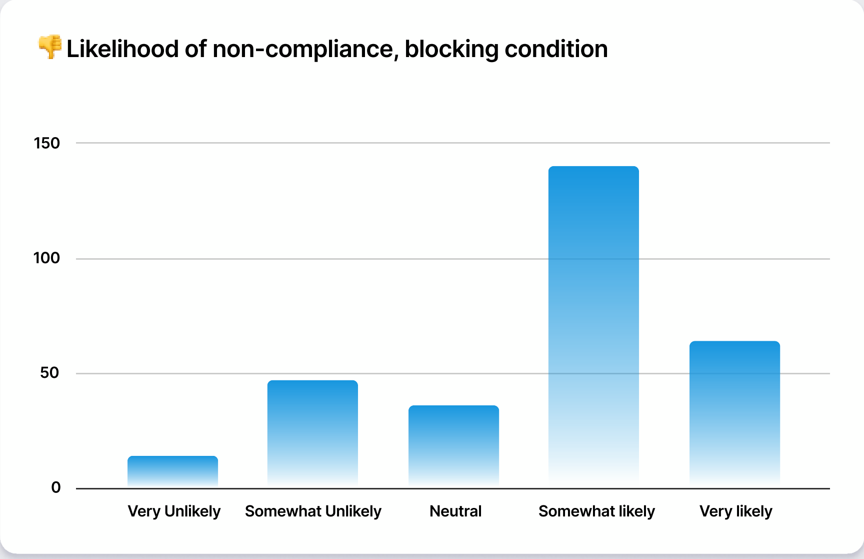
In the blocking condition, non-compliance was highly likely. Participants presented with a blocking intervention were twice as likely to look for a workaround than to abandon the effort altogether. **67%** of participants reported that they were somewhat or very likely to look for a workaround, while only **32%** said they would be somewhat or very likely to abandon the effort to access the application.



Survey Question

How likely would you be to look for an alternative way to access Docubox? (Non-comply)

1 = very unlikely
2 = somewhat unlikely
3 = neutral
4 = somewhat likely
5 = very likely



Survey Question

How likely would you be to look for an alternative way to access Docubox? (Non-comply)

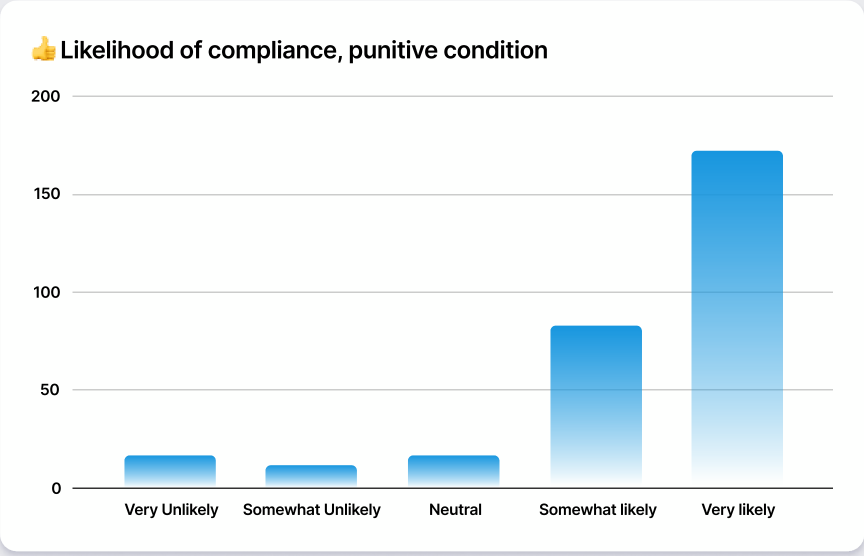
1 = very unlikely
2 = somewhat unlikely
3 = neutral
4 = somewhat likely
5 = very likely

Research notes

Participants report that they would likely look for an alternative way to access the application, on average (M = 3.64, $p < .001$).

Participants presented with a punitive intervention were also likely to comply with it.

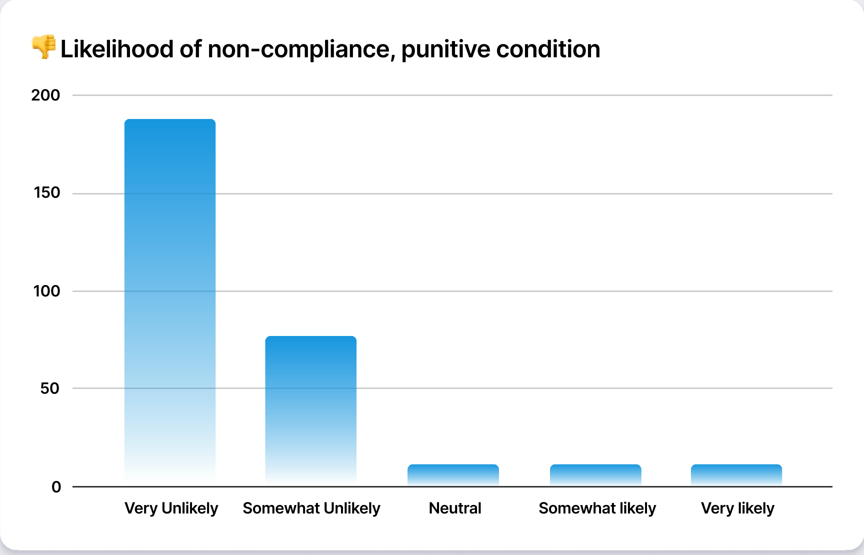
Surprisingly, in the punitive condition, participants said, on average, that they would be unlikely to ignore the message and that they would be likely to complete the training module.


👍 Likelihood of compliance, punitive condition

Survey Question

How likely would you be to ignore the message from IT? (Non-comply)

1 = very unlikely
2 = somewhat unlikely
3 = neutral
4 = somewhat likely
5 = very likely


👎 Likelihood of non-compliance, punitive condition

Survey Question

How likely would you be to complete the security training module within one week? (Comply)

1 = very unlikely
2 = somewhat unlikely
3 = neutral
4 = somewhat likely
5 = very likely

Research notes

In the punitive condition, participants said, on average, that they would be very unlikely to ignore the message (M = 1.61, p < .001) and that they would be likely to complete the training module (M = 4.27, p < .001).

Key Takeaway

Our results seem to validate what security practitioners have long claimed: that employees look for ways to circumvent their security blockades. Yet, when those blockades are lifted and replaced with non-disruptive, helpful security nudges and corrective interventions, people are more likely to oblige.

While participants in both the nudging intervention and punitive intervention reported that they were highly likely to comply with the intervention, it’s worth noting that security nudges engendered less negative opinions and feelings. In addition, security leaders should take into consideration the time expense of additional training sessions as well as the question of security fatigue that may result. Even Gartner has recently called into question the overall efficacy of conventional security training programs.

Results

Correlating attitudes, emotions and behaviors

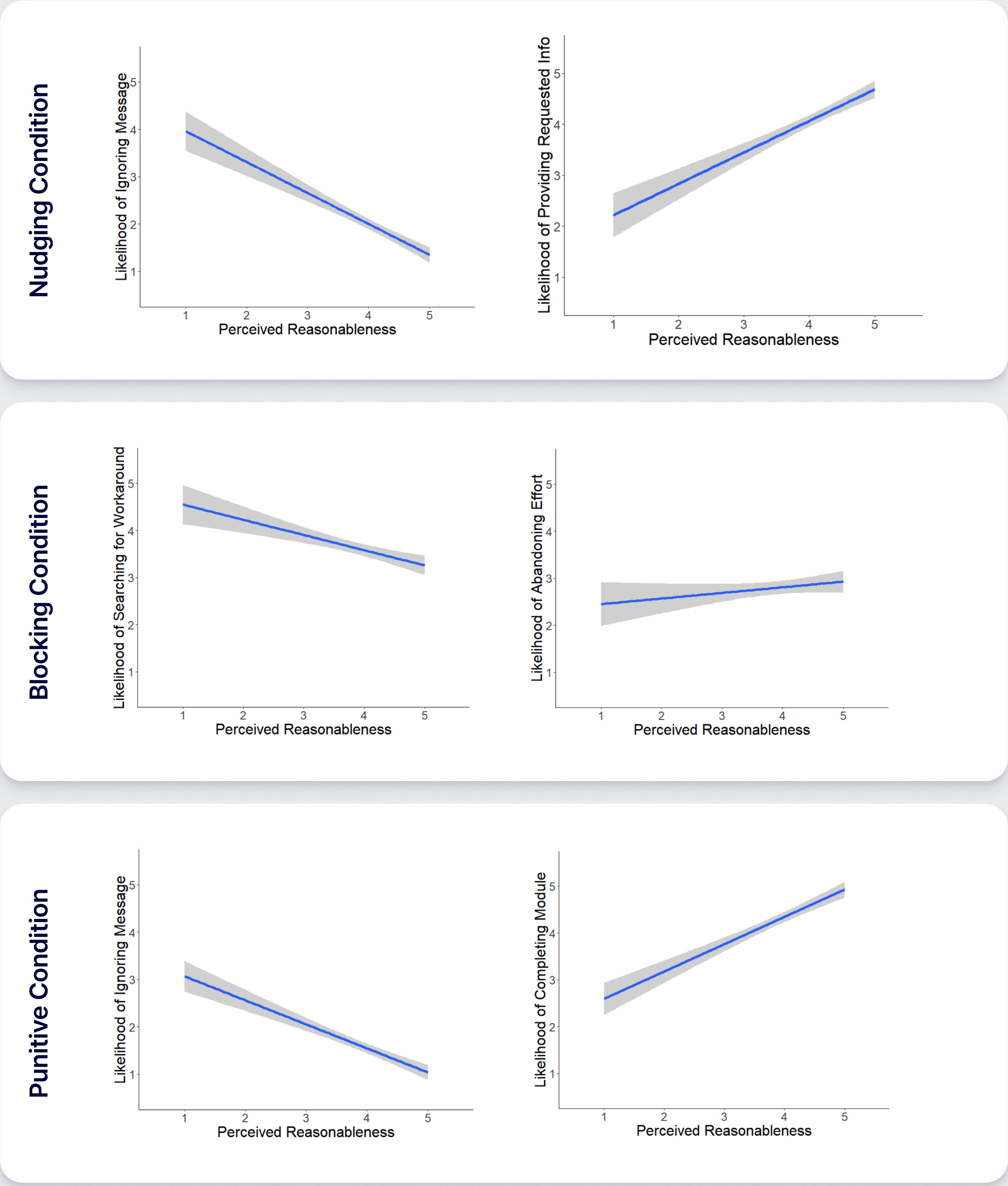
Overall, attitudes and emotions were strong indicators of security behaviors.

Across every condition in our experiment, we found statistically significant relationships between participants' attitudes and behaviors as well as their emotions and behaviors.

Across all conditions, perceived reasonableness was a strong indicator of compliance.

Within every experimental condition (blocking, nudging, punitive), the perceived reasonableness of the intervention predicted compliance. In the nudging condition, the more reasonable participants believed the intervention to be, the less likely they would be to ignore the message ($r = -.50$, $p < .001$) and the more likely they would be to respond to the message with the information requested ($r = .47$, $p < .001$). In the blocking condition, the more reasonable participants believed the intervention to be, the less likely they were to look for an alternative way to access the blocked application ($r = -.25$, $p < .001$). In the punitive condition, the more reasonable participants believed the intervention to be, the less likely they would be to ignore the message ($r = -.48$, $p < .001$) and the more likely they would be to complete the training module ($r = .50$, $p < .001$).

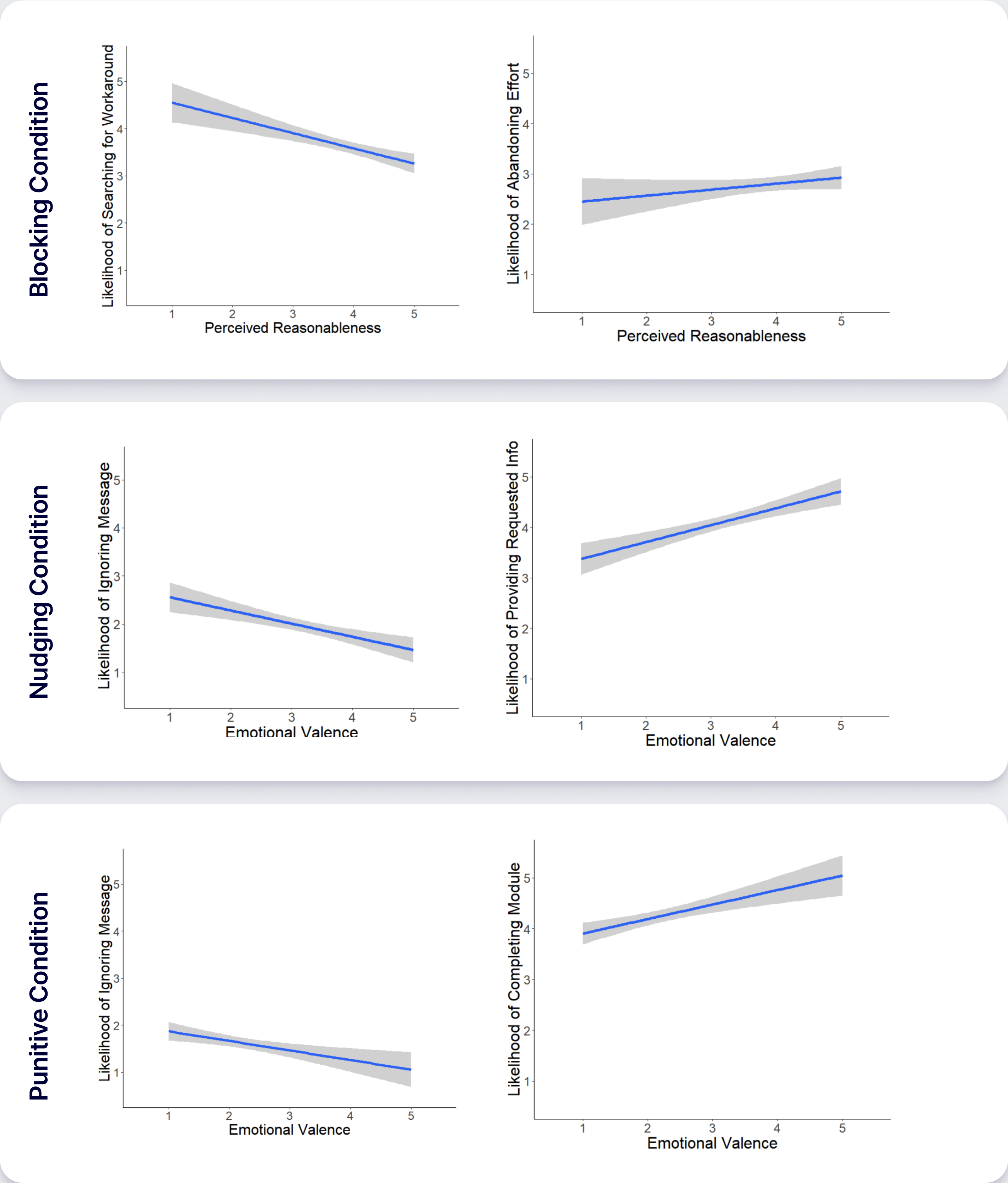
Perceived reasonableness and likelihood of compliance, correlation



Across all conditions, emotion was a strong indicator of compliance.

Within each experimental condition (blocking, nudging, punitive), participants' emotional reactions to the intervention predicted compliance. In the nudging condition, the more negatively participants reacted, the more likely they would be to ignore the message ($r = -.24$, $p < .001$) and the less likely they would be to respond to the message with the information requested ($r = .28$, $p < .001$). In the blocking condition, the more negatively participants reacted, the more likely they were to look for an alternative way to access the blocked application ($r = -.21$, $p < .001$). In the punitive condition, the more negatively participants reacted, the less likely they would be to ignore the message ($r = -.18$, $p = .003$) and the more likely they would be to complete the training module ($r = .23$, $p < .001$).

Emotional valence and likelihood of compliance, correlation



Key Takeaway

As articulated throughout this report, security leaders must take into consideration how their workforces feel about the controls and policies they develop. It is not only a matter of winning hearts and minds (which would be a nice residual benefit in a profession particularly prone to burnout), but also a matter of efficacy. No matter what types of security interventions or experiences security leaders create, they would be wise to bear in mind the old adage, “you can catch more flies with honey than with vinegar.”

About Nudge Security

Nudge Security is transforming the human element of cybersecurity. We believe that every employee is capable and open to making decisions that support and strengthen the organization's cyber risk posture. Our technology platform discovers and inventories every cloud and SaaS account employees create with zero reliance on network infrastructure, endpoint agents, or browser extensions. Using this info, security teams can nudge employees towards better decisions and behaviors as they adopt and use new SaaS and cloud technologies.

Nudge Security is available to organizations of all shapes and sizes with a free 14-day trial.

Start your trial now →

We are eager to engage with development and research partners to further study how security nudges can help to drive better security behaviors and outcomes within your organization. If you are interested in working with us on future research projects, please contact us at research@nudgesecurity.com.

Nudge Security was founded in 2021 by Jaime Blasco and Russell Spitler. The company secured funding led by Ballistic Ventures in 2022. Nudge Security is a fully remote company with outposts in Austin, Texas and Jackson, Wyoming. For more information, visit www.nudgesecurity.com

Follow us on Twitter
Follow us on LinkedIn