It's Not What You Know, It's What You Do: How Data Can Shape Security Engagement

Aika Sengirbay

Security Awareness Program Manager

Airbnb

Masha Sedova

Co-Founder

Elevate Security

@ModMasha

ABOUT AIKA SENGIRBAY

Trained in Cyber Security

Building Security Awareness Programs for General and Technical communities

Background in Incident Response & Red Team

Passionate about building **security culture**

ABOUT MASHA SEDOVA

I play at the intersection of computer security & behavioral science

Elevate Security

Co-Founder, building the Behavioral Security Platform

salesforce

Built and ran Salesforce trust engagement team

Passionate about transforming security behaviors from “have to” to “want to”

TRANSFORM EVERY EMPLOYEE TO SECURITY SUPERHUMAN

95% OF DATA BREACHES ARE CAUSED BY THE HUMAN FACTOR

WHY THE OLD WAY WAS BROKEN

PREVIOUS STATE

Compliance

Check the box security

One Size Fits All

Same training for everyone

Unquantified

Unmeasured, no improvements

No Replay-ability

Not dynamic, no personalization, heavy churn

THE RESULT

Disengaged

Poor choices

No change

NEW METHODOLOGY -> NEW GOALS

1. Make it relevant
2. Recognize employee’s existing skill level
3. Respect employee’s time
4. Recognize employee’s progress
5. Motivate further improvement

WHAT DID WE DECIDE TO BUILD?

WE BUILT

THE INDIVIDUAL SECURITY SNAPSHOT

1. **Focuses on your prioritized security behaviors**
2. **Identifies individual strengths and weaknesses**
3. **Provides individualized recommendations for training**
4. **Rewards when successful**

THE CREATION PROCESS

STEP 1
CREATE MASTER LIST OF DESIRED BEHAVIORS

THE MASTER LIST

Sensitive Data Handling

Using Password Managers

Patching

Phishing Susceptibility

Increase Reporting

Malware Infection

2FA Adoption

USB Usage

VPN Usage

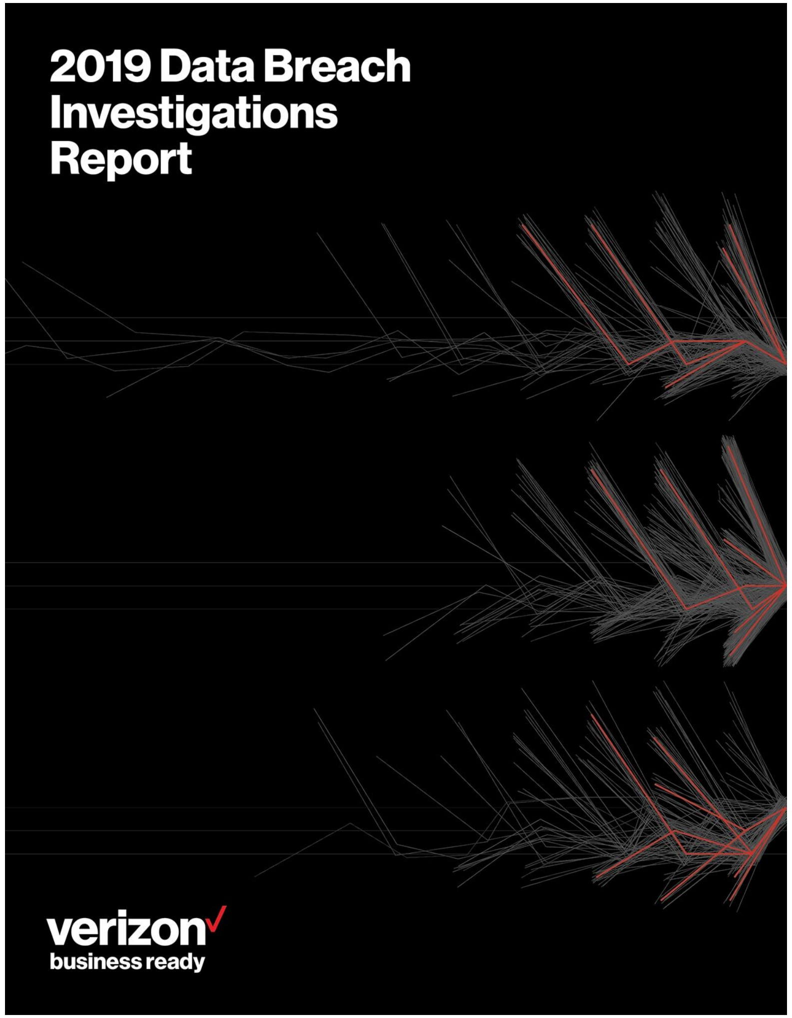
Safe Browsing

STEP 2
PRIORITIZE VITAL BEHAVIORS

PRIORITIZE BEHAVIORS

1. What are your most frequent incidents?
2. What would be the most damaging to your company?
3. What are easy wins?
4. What’s the most visible?
5. What would have the greatest impact on your security posture?
6. What does your team already have metrics on?
7. What do your stakeholders care most about?

USE THREAT INTELLIGENCE TO PRIORITIZE



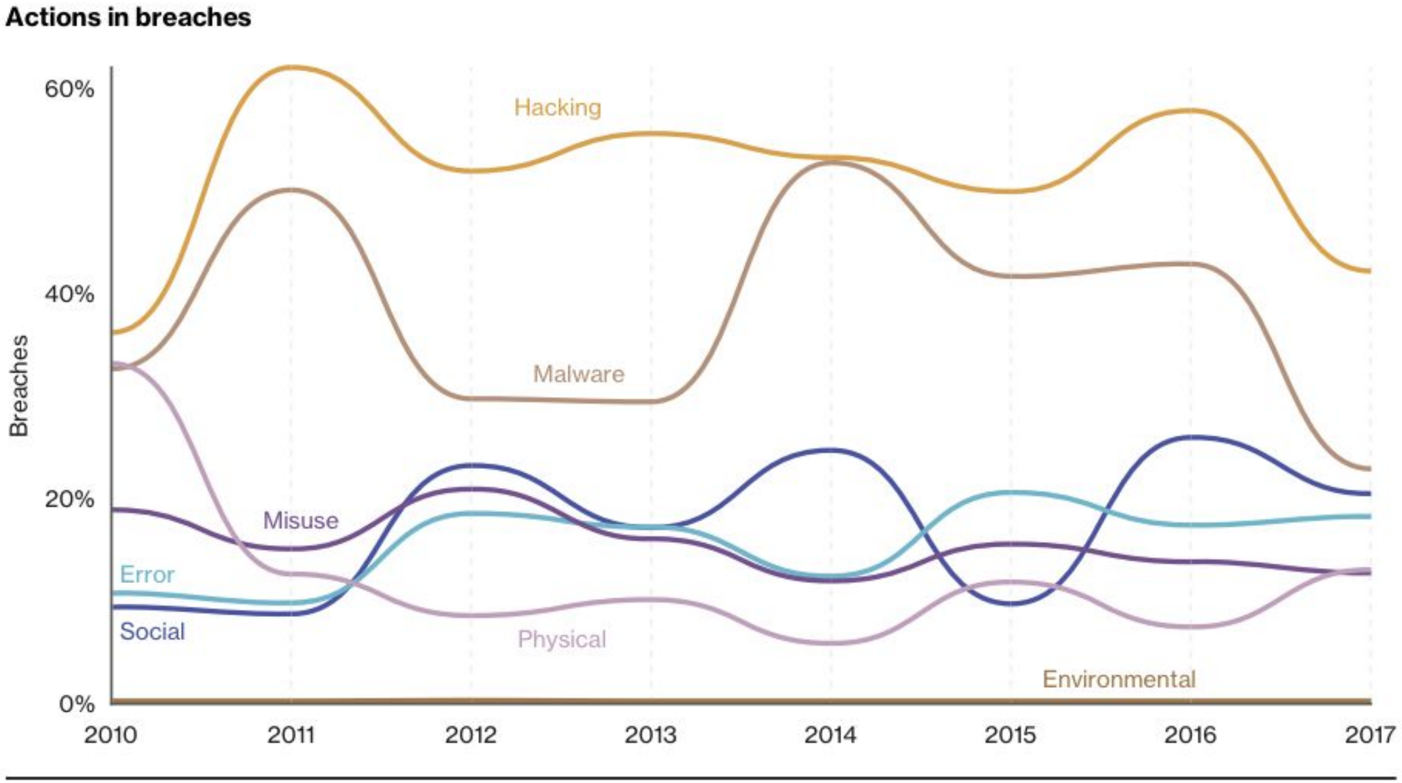
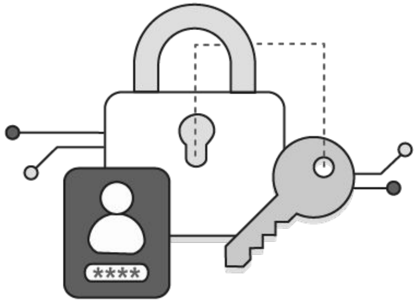


Figure 3. Percentage of breaches per threat action category over time

EXAMPLE OF TOP SECURITY BEHAVIORS

Phishing - compromised creds



Password management adoption

Reporting suspicious emails

Training

STEP 3
FINDING THE DATA

DATASETS

Phishing:

run internal assessments

Reporting suspicious emails:

work closely with IR & email teams

Passwords Management:

pull from the enterprise device admin

Training completion:

pull from Learning Management Tool

STEP 4
DEFINE THE INDIVIDUAL’S SUCCESS

DEFINING SUCCESS

Phishing:

No compromised credentials

Reporting:

Sent in a report via appropriate channels

Passwords Management:

Installed

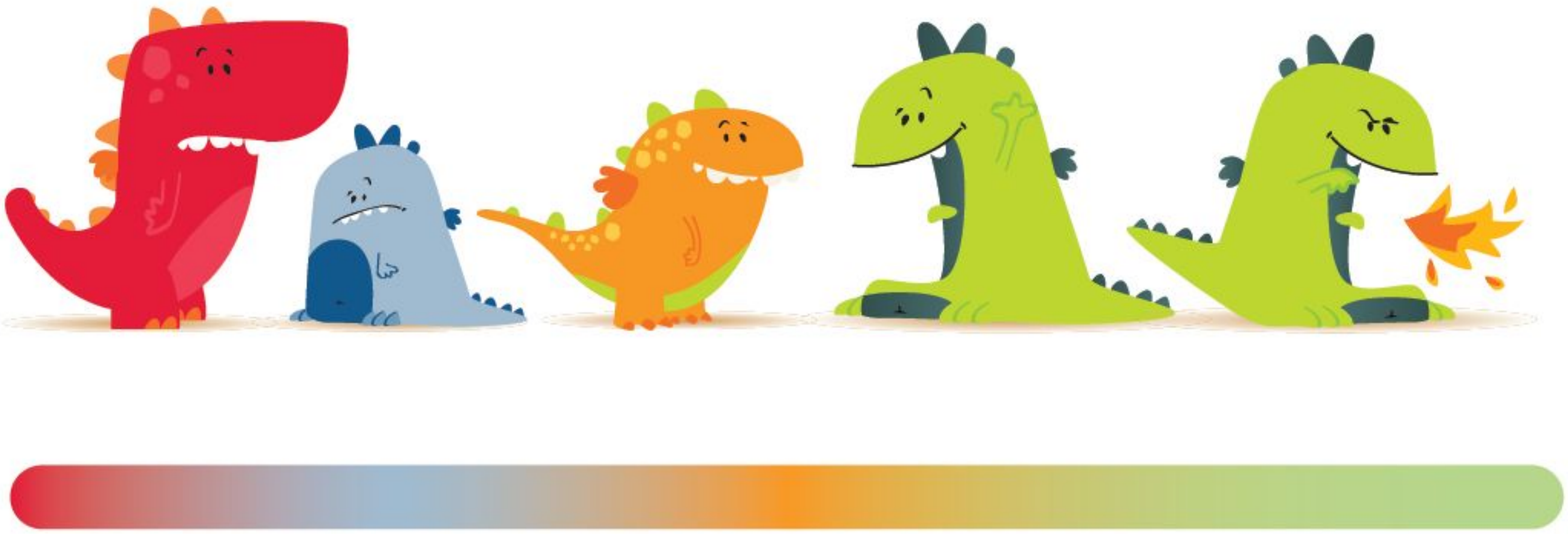
Active (in the last 30 days)

Training completion:

Completed

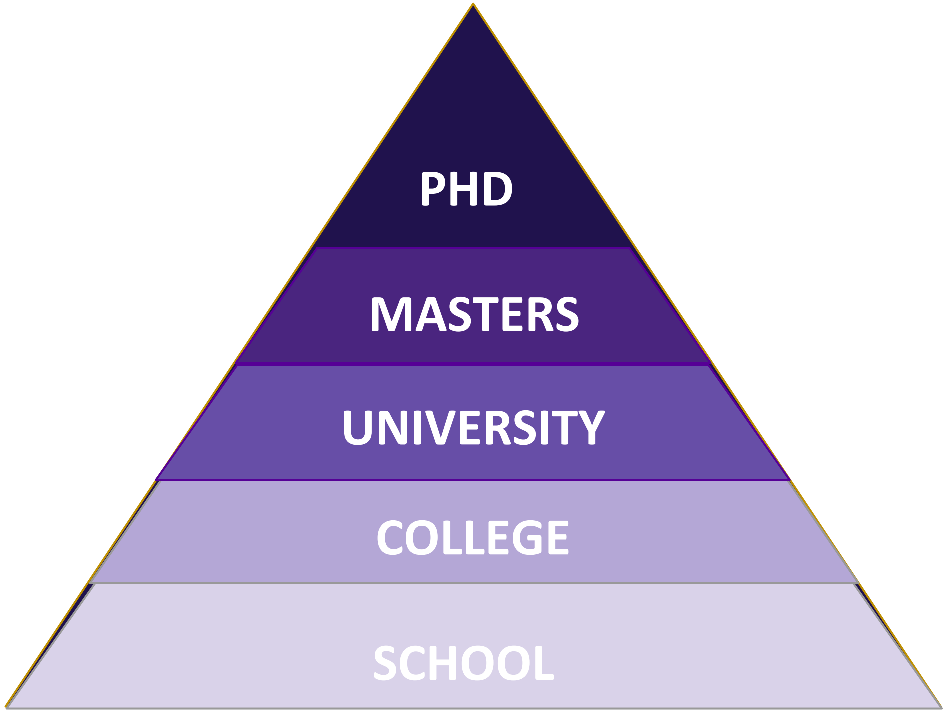
STEP 5
DESIGNING FOR:
CULTURAL RELEVANCE,
THE FUTURE,
IMPACT

DESIGN: STATIC VS. DYNAMIC

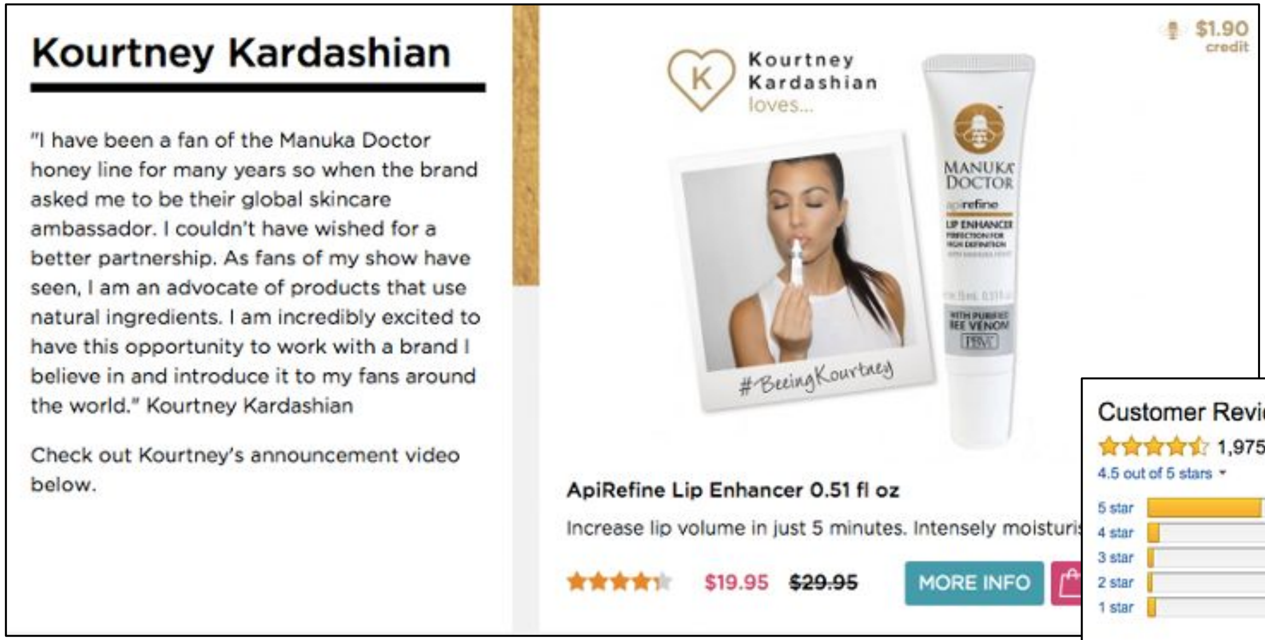


Flimsy Tenuous Sturdy Fortified Indestructible

EDUCATION LEVELS (STATIC) VS. CREDIT SCORE (DYNAMIC)



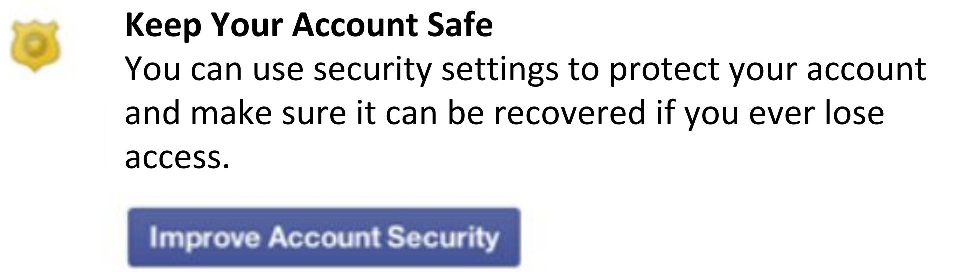
THE POWER OF SOCIAL PROOF



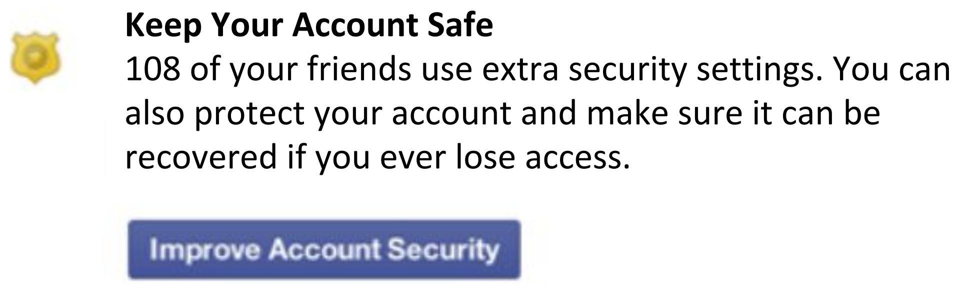
SOCIAL PROOF IN SECURITY

The study of Sauvik Das of Georgia Institute of Technology found that a Facebook prompt to install security controls was **1.36x** more successful when using social proof.

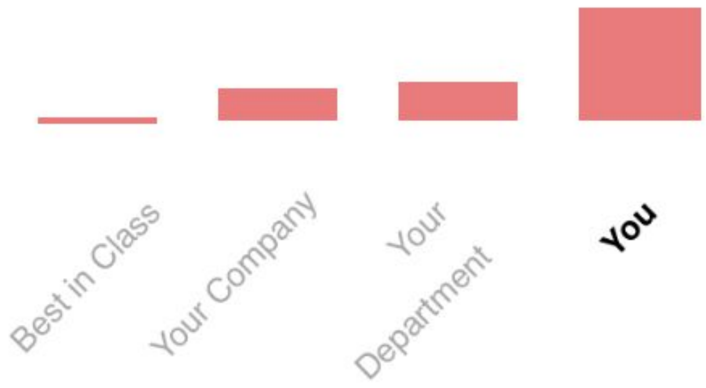
Control



Social Context



COMPROMISED



Oh no! You are **3.2 times** more likely to fall for a phish and submit your credentials than people in your department. You can do better!

Strengthen skills

LastPass Use

Password managers are the best way to have unique and strong passwords across all your accounts - both personal and work!

12% of your department has installed LastPass

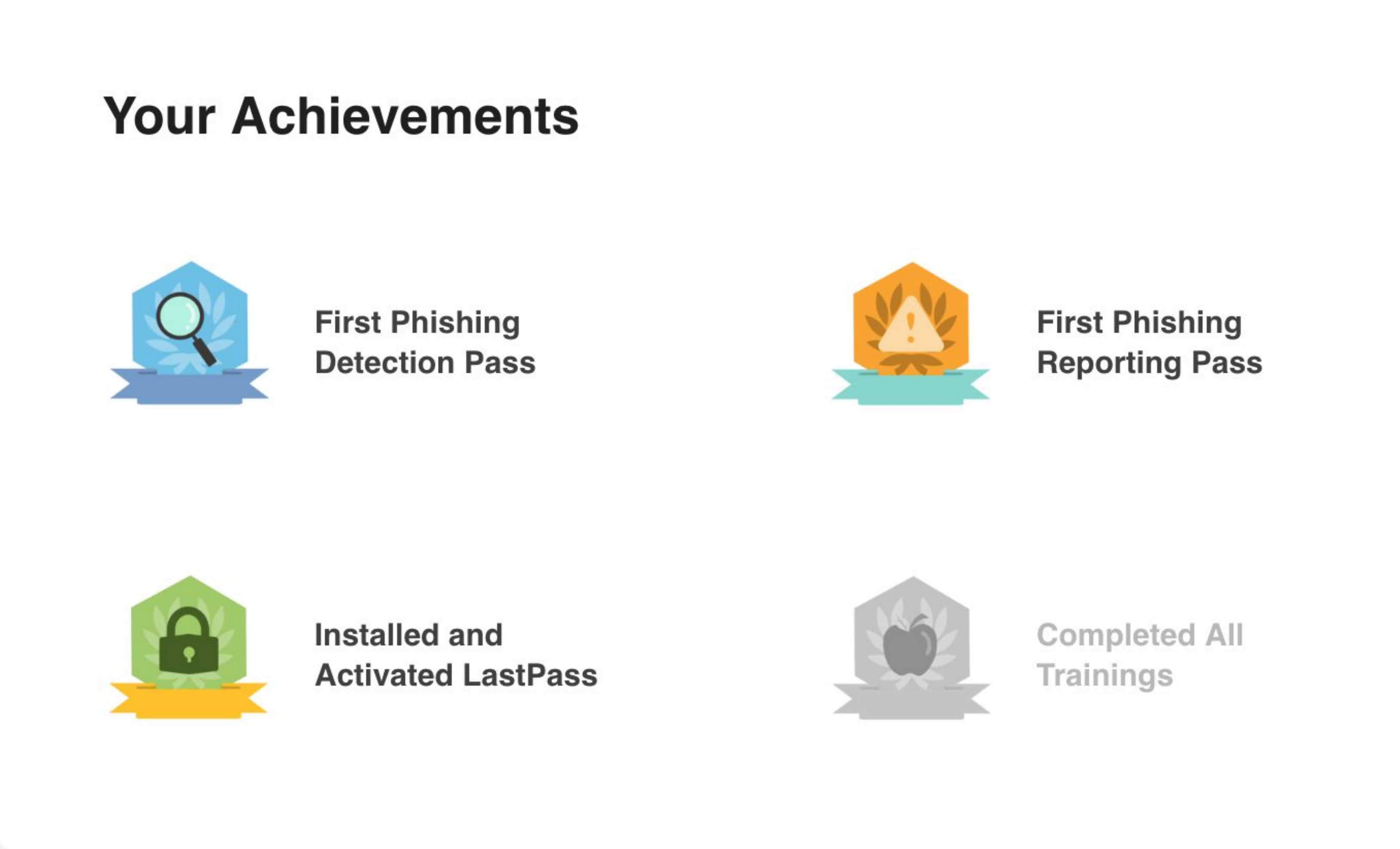
Installed LastPass

Used LastPass

Autodesk CEO Andrew Anagnost uses LastPass too!

You earned a badge!

INTRINSIC MOTIVATION- ACHIEVEMENT



SHOW ME THE SNAPSHOT

Here's your

SECURITY SNAPSHOT

Keep up the good work!

Nice Work!

You're **Indestructible**! The rest of your company is Sturdy. Thank you for doing your part to keep Autodesk safe.

Flimsy Tenuous Sturdy Fortified Indestructible

Here's your

SECURITY SNAPSHOT

Make all your red sections green, and you'll be **Indestructible** in no time!

Eeeek!

You're **Flimsy**. The rest of your company is Sturdy. Your security skills need some attention to keep you and Autodesk secure.

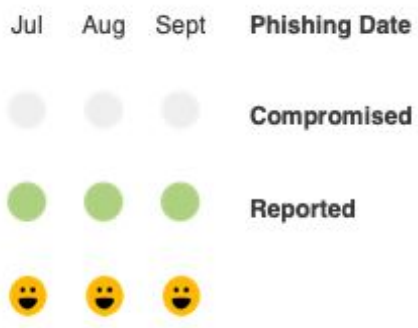
Flimsy Tenuous Sturdy Fortified Indestructible

HERE'S A BREAKDOWN:

Phishing & Reporting

Over the last quarter, we've sent you a few mock phishing emails to see if you were able to detect them!

Phishing is the fraudulent practice of sending malicious emails that try to steal your credentials or download malicious software.



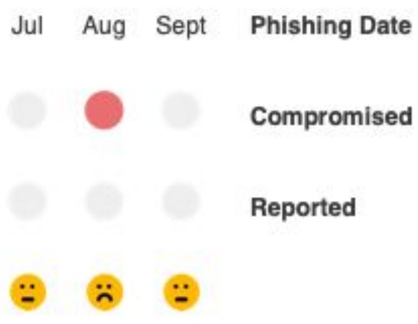
Review tests

HERE'S A BREAKDOWN:

Phishing & Reporting

Over the last quarter, we've sent you a few mock phishing emails to see if you were able to detect them!

Phishing is the fraudulent practice of sending malicious emails that try to steal your credentials or download malicious software.



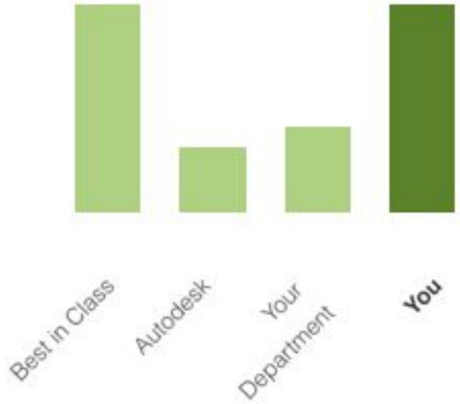
Review tests

COMPROMISED

You detected **all** of the phishing emails this quarter! Good job!

You earned a badge!

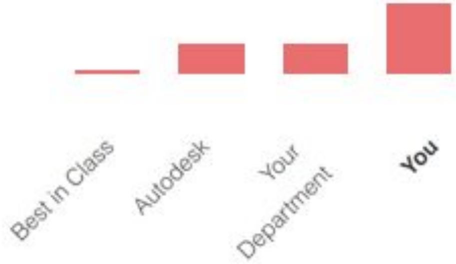
REPORTED



Good job! You're **2.5 times** more likely to report than the rest of your department!

You earned a badge!

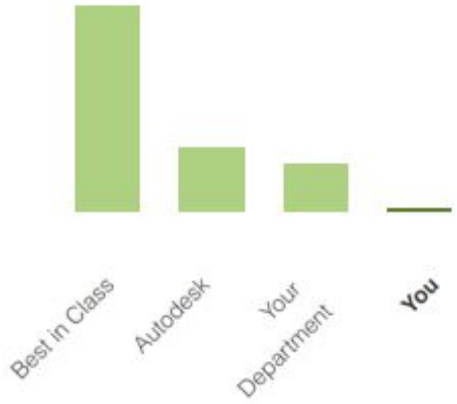
COMPROMISED



Oh no! You are **2.6 times** more likely to fall for a phish and submit your credentials than people in your department. You can do better!

Strengthen skills

REPORTED



While your department reported 21.9% of the links, you didn't report any. You can do better!

Learn to report

LastPass Use

Password managers are the best way to have unique and strong passwords across all your accounts.

Autodesk CEO Andrew Anagnost uses LastPass too!

You earned a badge!

15.6% of your department has installed LastPass

Installed LastPass

LastPass Use

Snapshot recommends installing LastPass before a company-wide rollout in Q1.

Autodesk CEO Andrew Anagnost uses LastPass. You should too!

Install LastPass

15.6% of your department has installed LastPass

Installed LastPass

Trainings Done

In order for us to meet our compliance requirement to auditors and customers, every employee is required to complete an annual security training.

89% of your department has completed their trainings

Annual Security Training

You earned a badge!

Trainings Done

In order for us to meet our compliance requirement to auditors and customers, every employee is required to complete an annual security training.

89.3% of your department has completed their trainings

Annual Security Training

Sign up for Trainings

Your Achievements

First Phishing Detection Pass

First Phishing Reporting Pass

Installed LastPass

Completed Required Training

Your Achievements

First Phishing Detection Pass

First Phishing Reporting Pass

Installed LastPass

Completed Required Training

AFTER THE LAUNCH

QUALITATIVE RESULTS

60%

REVIEWED SNAPSHOT

89%

ENJOYED SEEING SNAPSHOT

83%

THE INFORMATION PRESENTED IN A CLEAR WAY

84%

MOTIVATED TO CHANGE SECURITY BEHAVIORS & INTERESTED TO LEARN MORE ABOUT SECURITY

SURVEY FEEDBACK

“This is the best security email ever! I really love the initiative. Clear, gives me an idea of where I stand and helps me see what else I can do. Plus, I can rub my colleagues noses in it a bit :P “

“I didn't realise that I had to report phishing emails...will do going forward “

“It's really fun, and I'm happy to be earning achievements. Really appeals to the gamer in me!“

“Great, simple and concise overview. If this eventually replaced one off annual training as well, you'd have won in my eyes”

TIME SAVING

Reported:

60% of company demonstrated “successful” criteria and didn’t need the training

445 hours saved

Phishing:

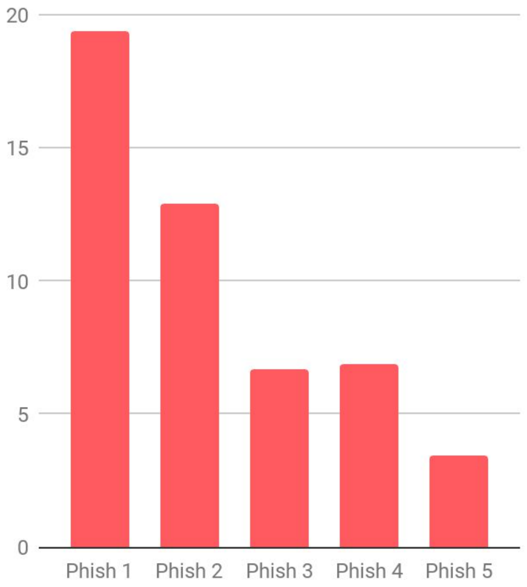
69% of the company successfully withstood giving up their credentials and didn’t need the the training.

512 hours saved

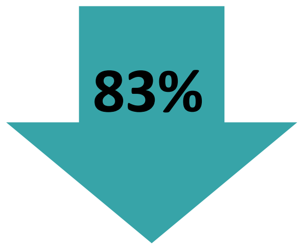
YEAH THAT'S COOL,

BUT DID IT WORK..?

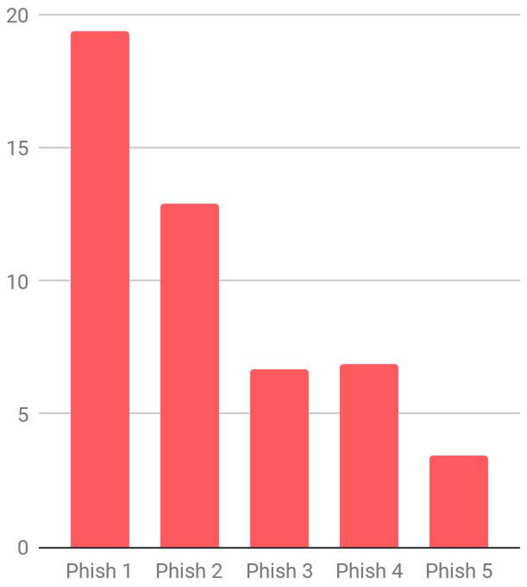
BEHAVIORS IMPROVED



Compromised

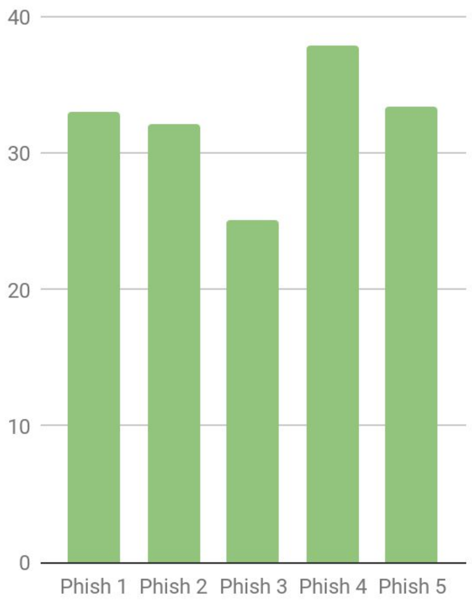


BEHAVIORS IMPROVED



Compromised

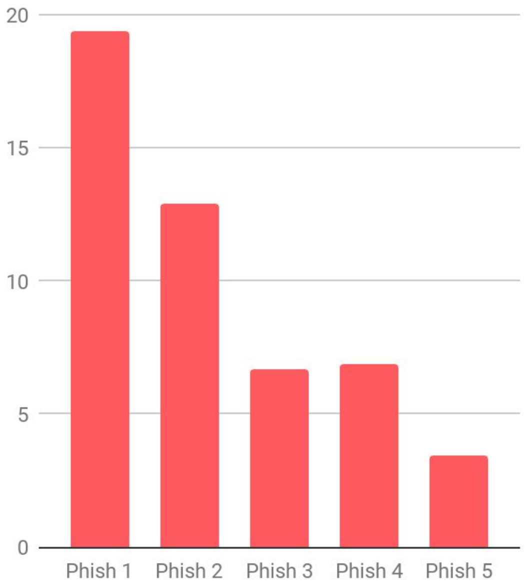
83%



Reporting

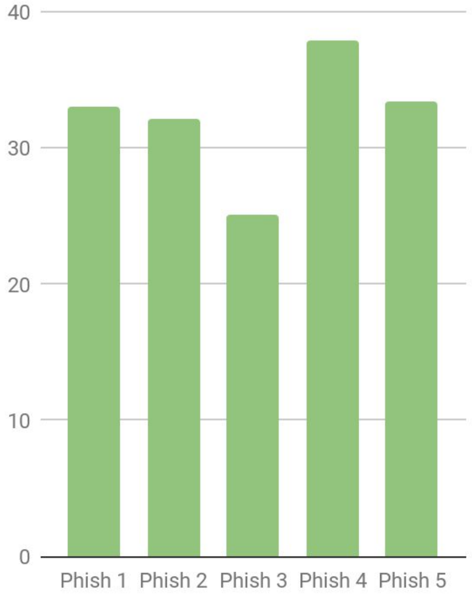
32%

BEHAVIORS IMPROVED



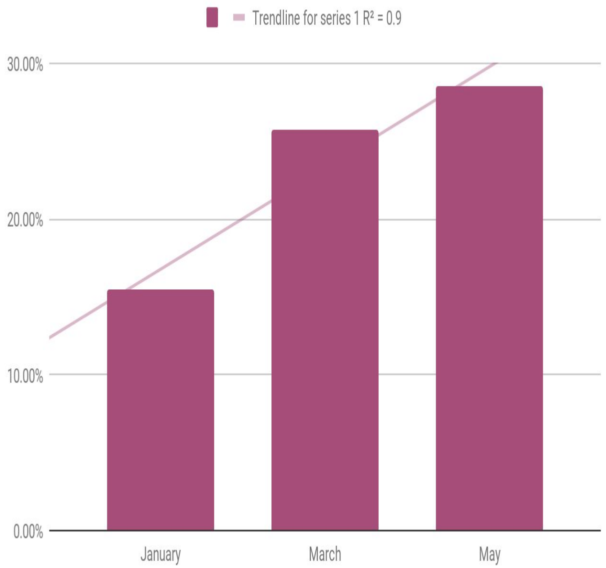
Compromised

83%



Reporting

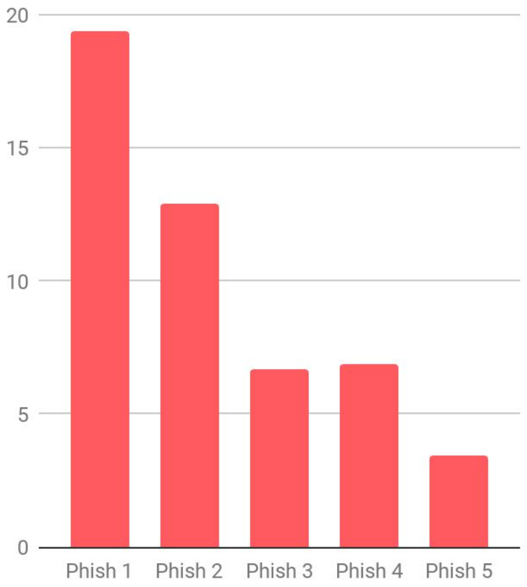
32%



Lastpass Adoption

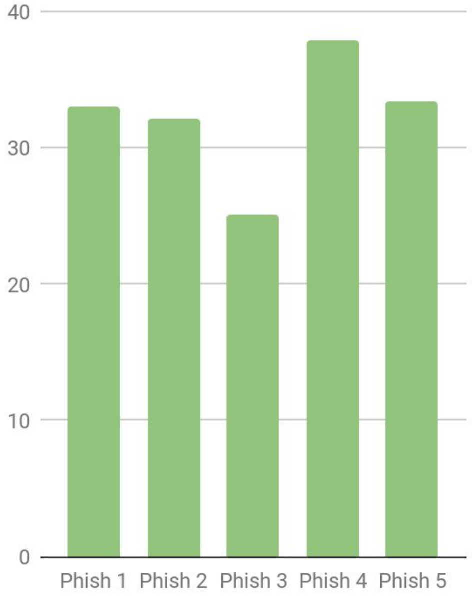
87%

BEHAVIORS IMPROVED



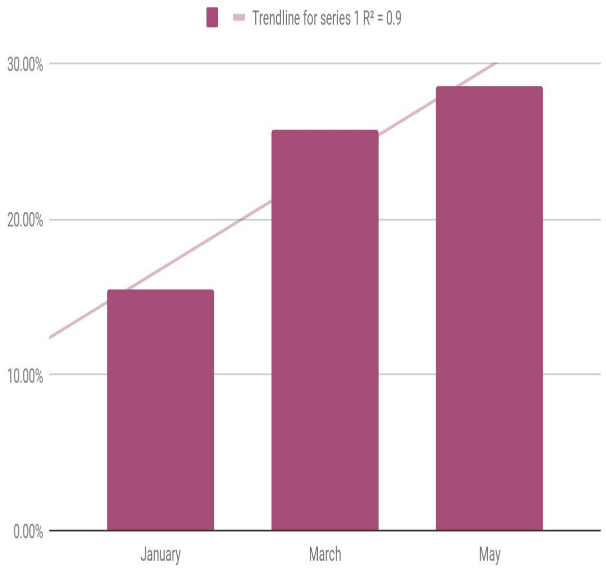
Compromised

83%



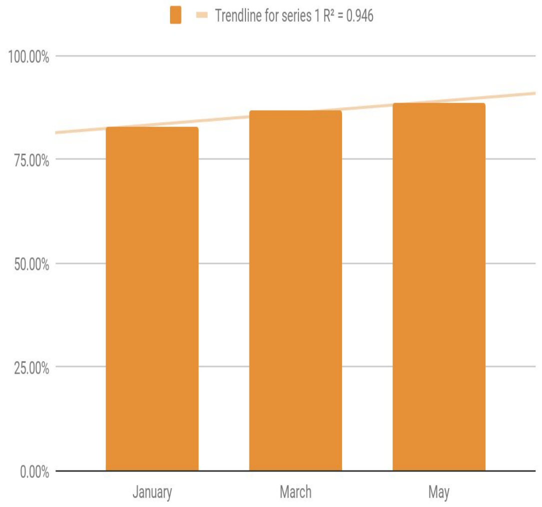
Reporting

32%



Lastpass Adoption

87%



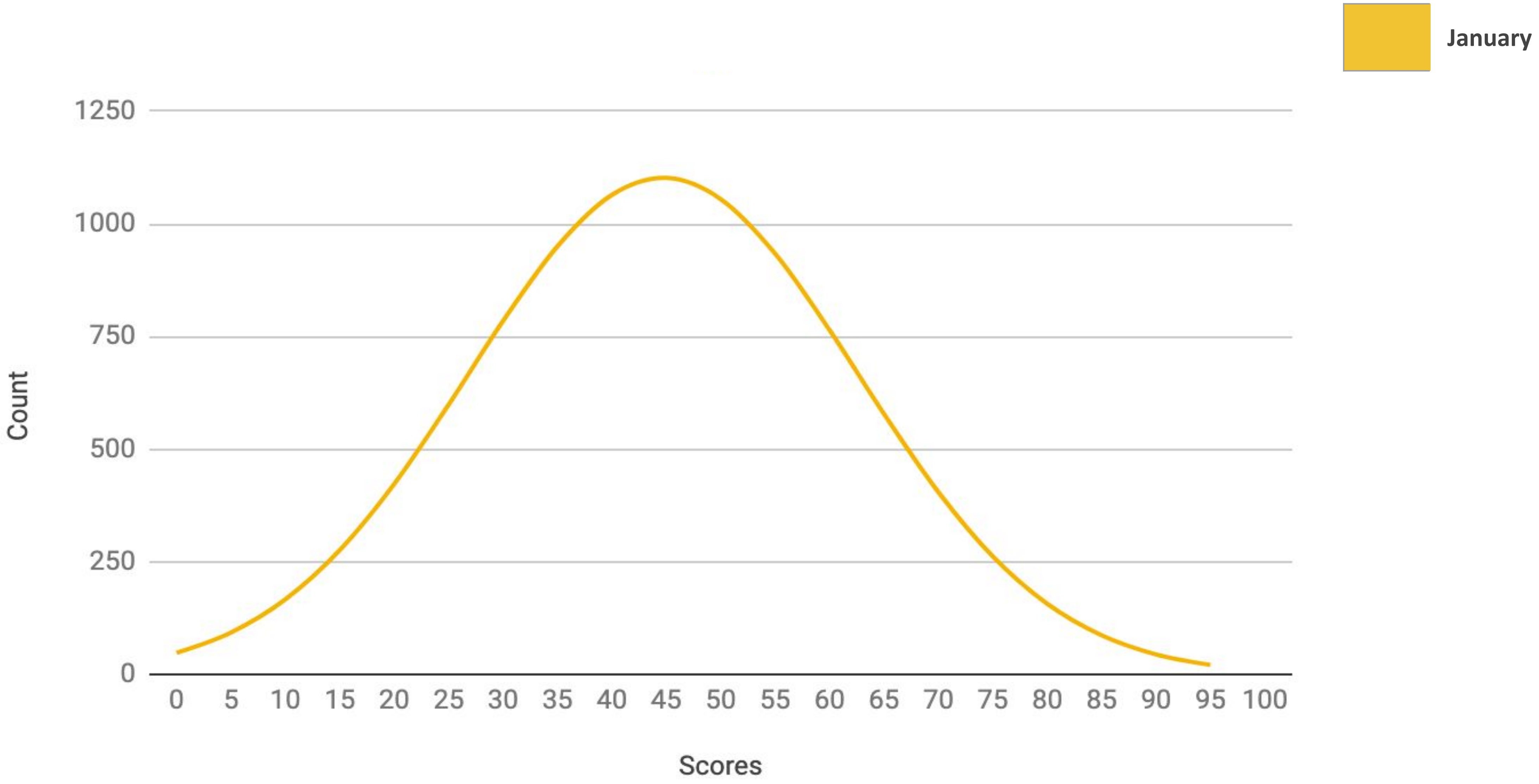
Training Completion

7%

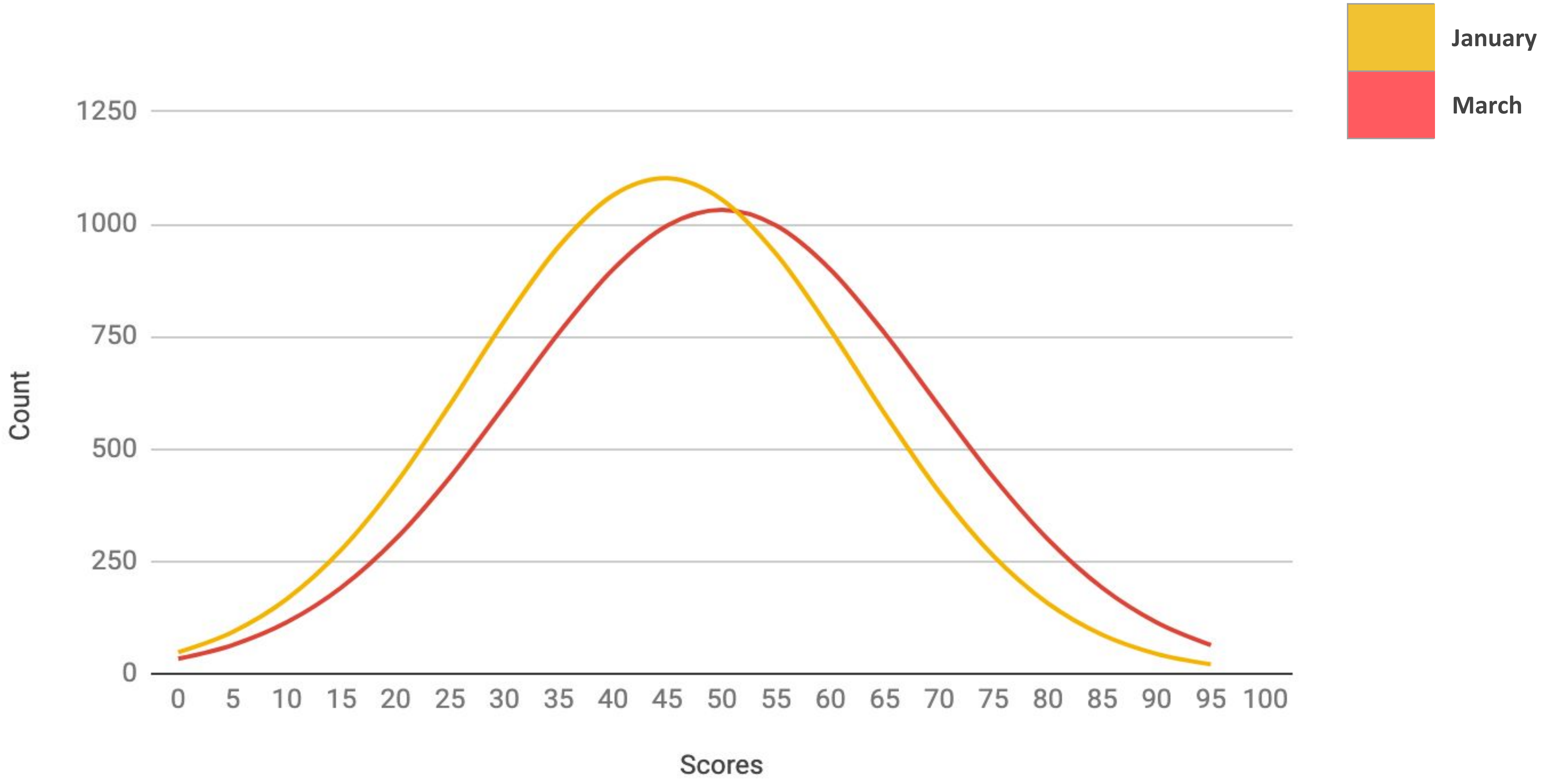
EVERY PULSE EMAIL SENT

IMPROVED THE AVERAGE SECURITY SCORE

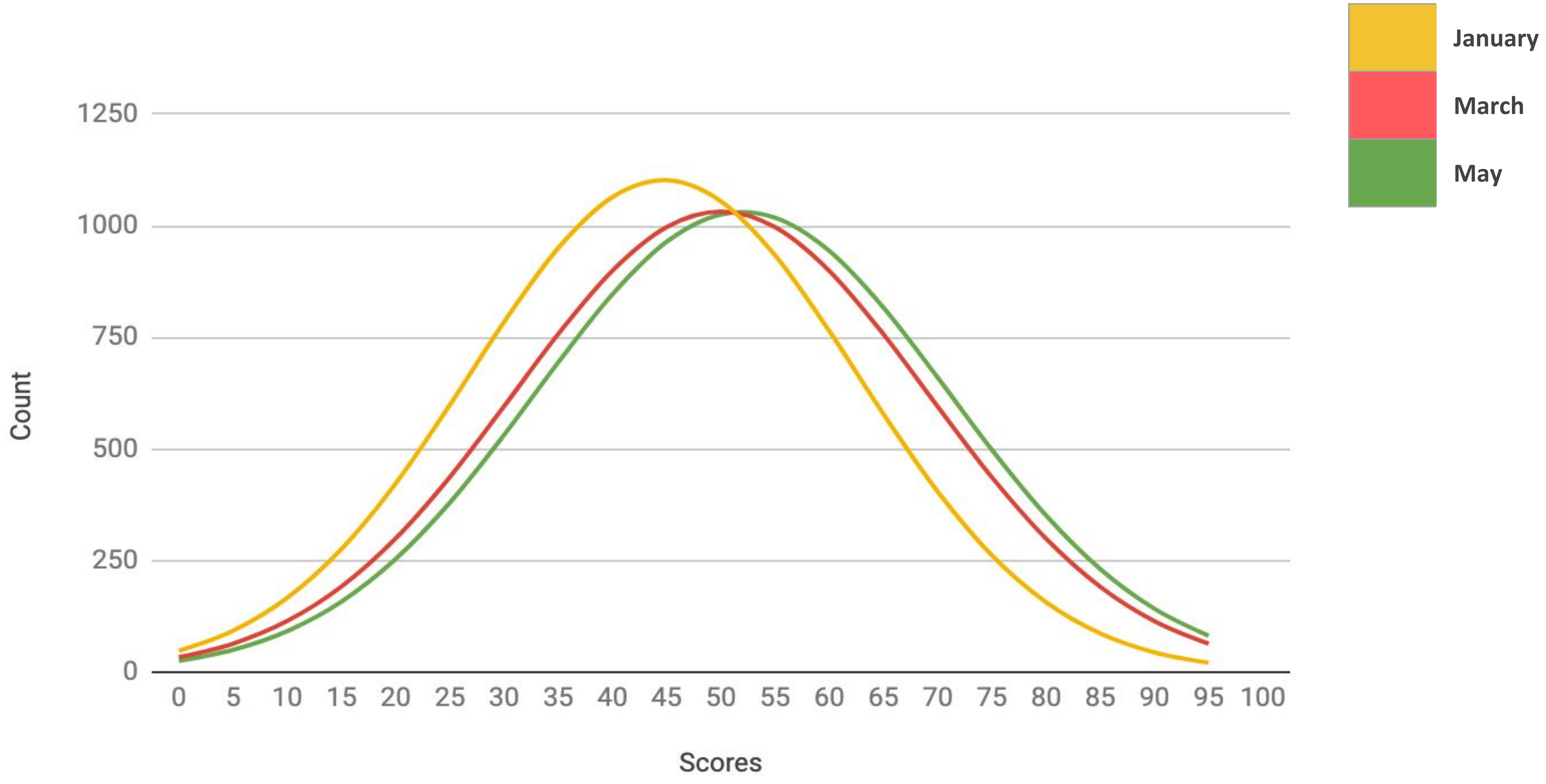
THE AVERAGE SECURITY SCORE

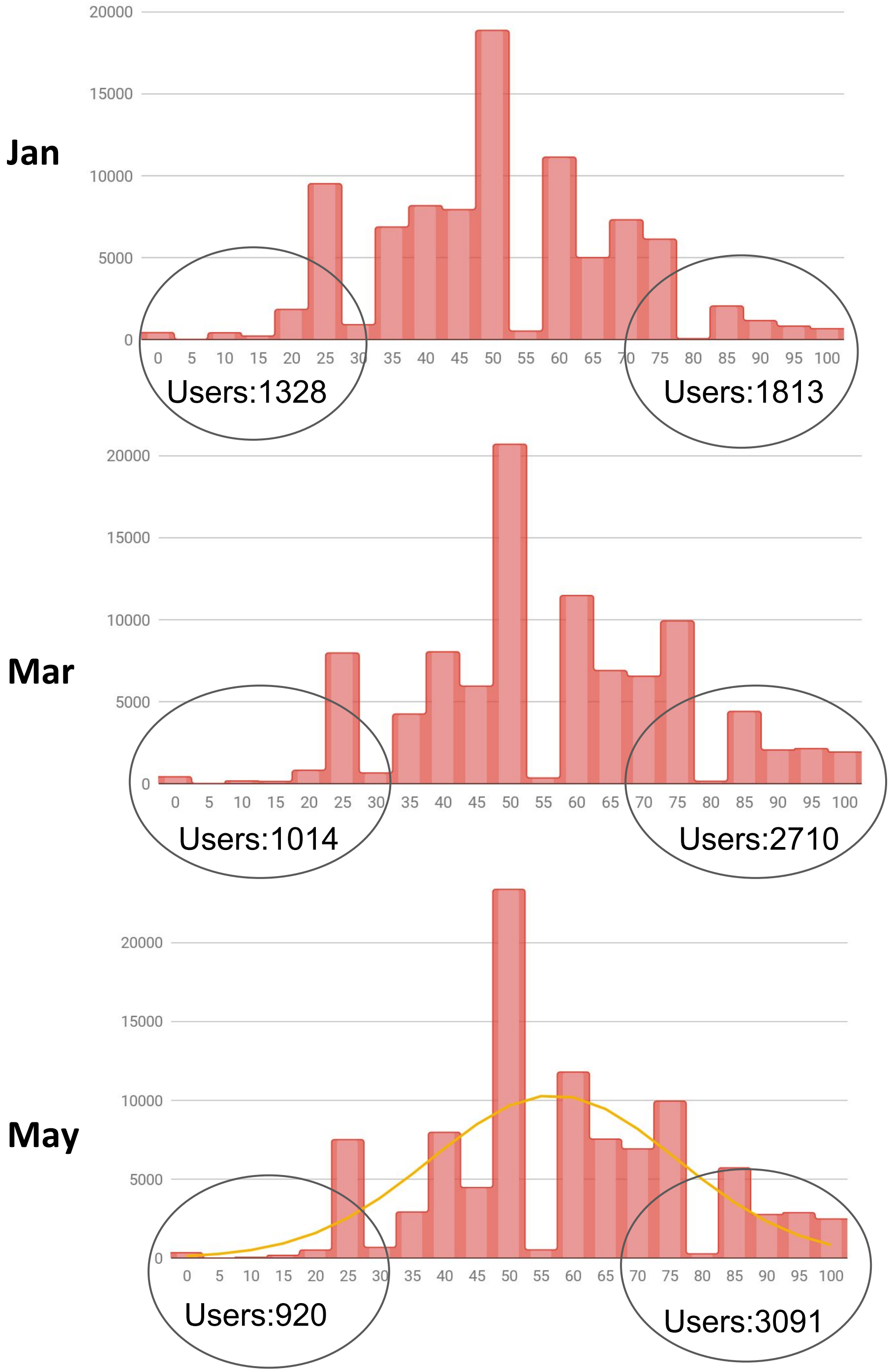


THE AVERAGE SECURITY SCORE



THE AVERAGE SECURITY SCORE

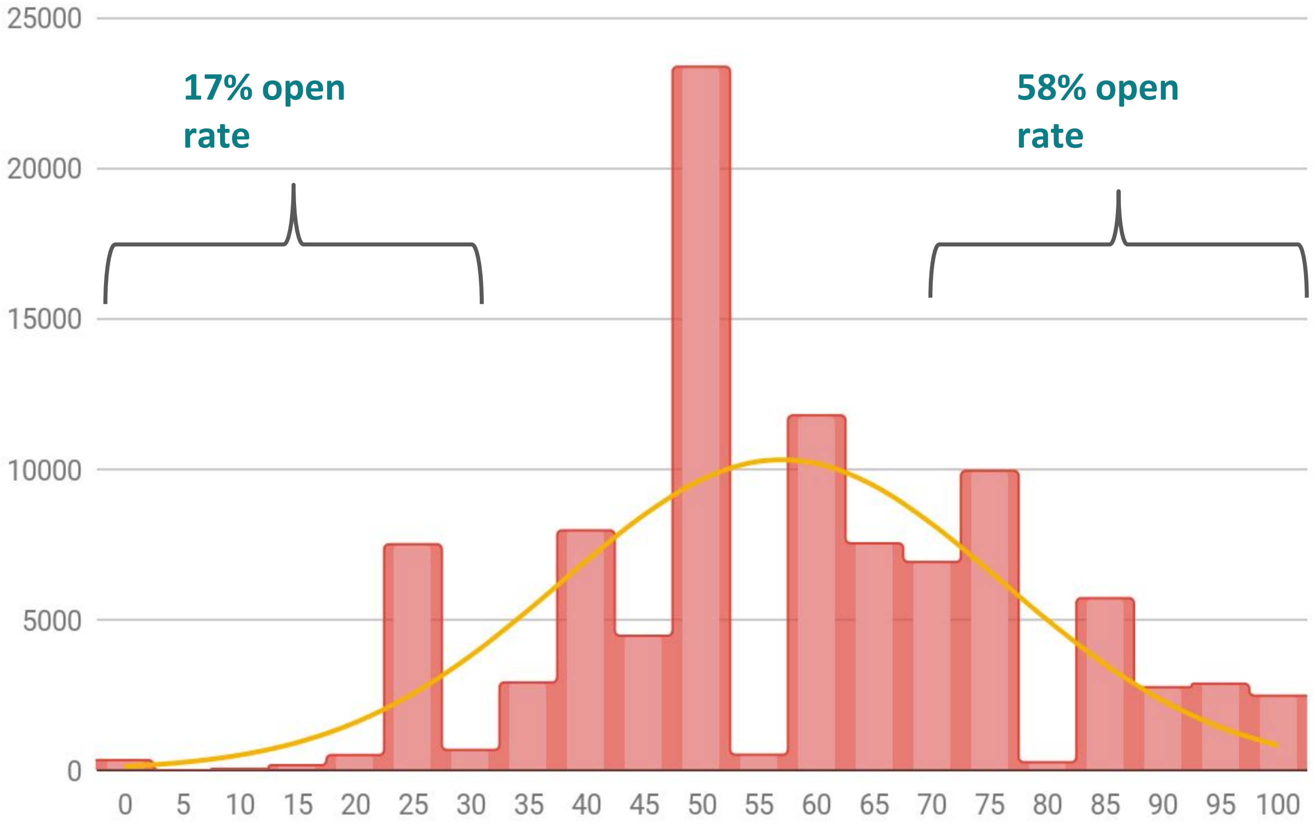




170% increase in top performers

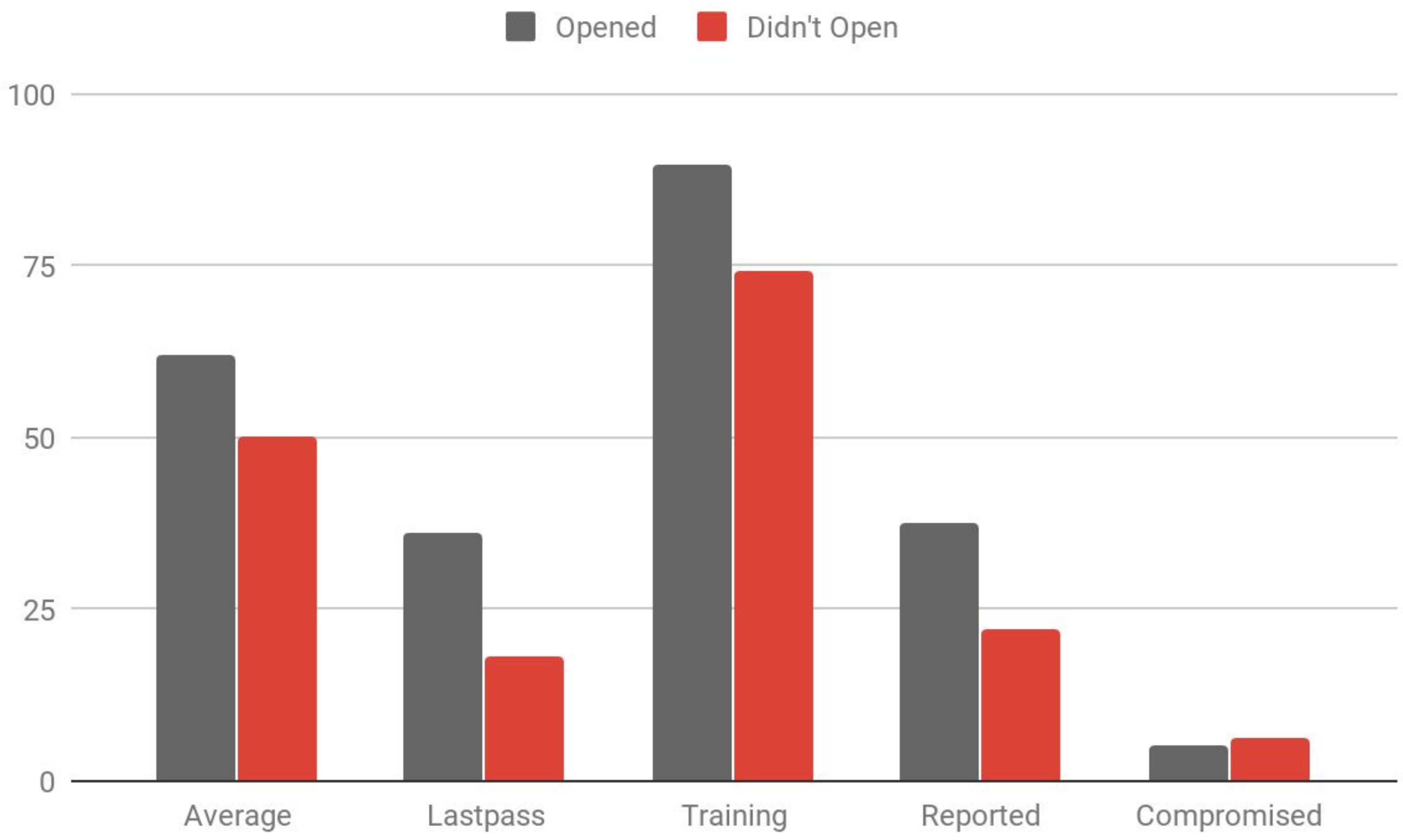
31% decrease in low performers

SAW VS. MISSED SNAPSHOT



People who had low behaviors scores also ignored the emails.

SAW VS. MISSED SNAPSHOT

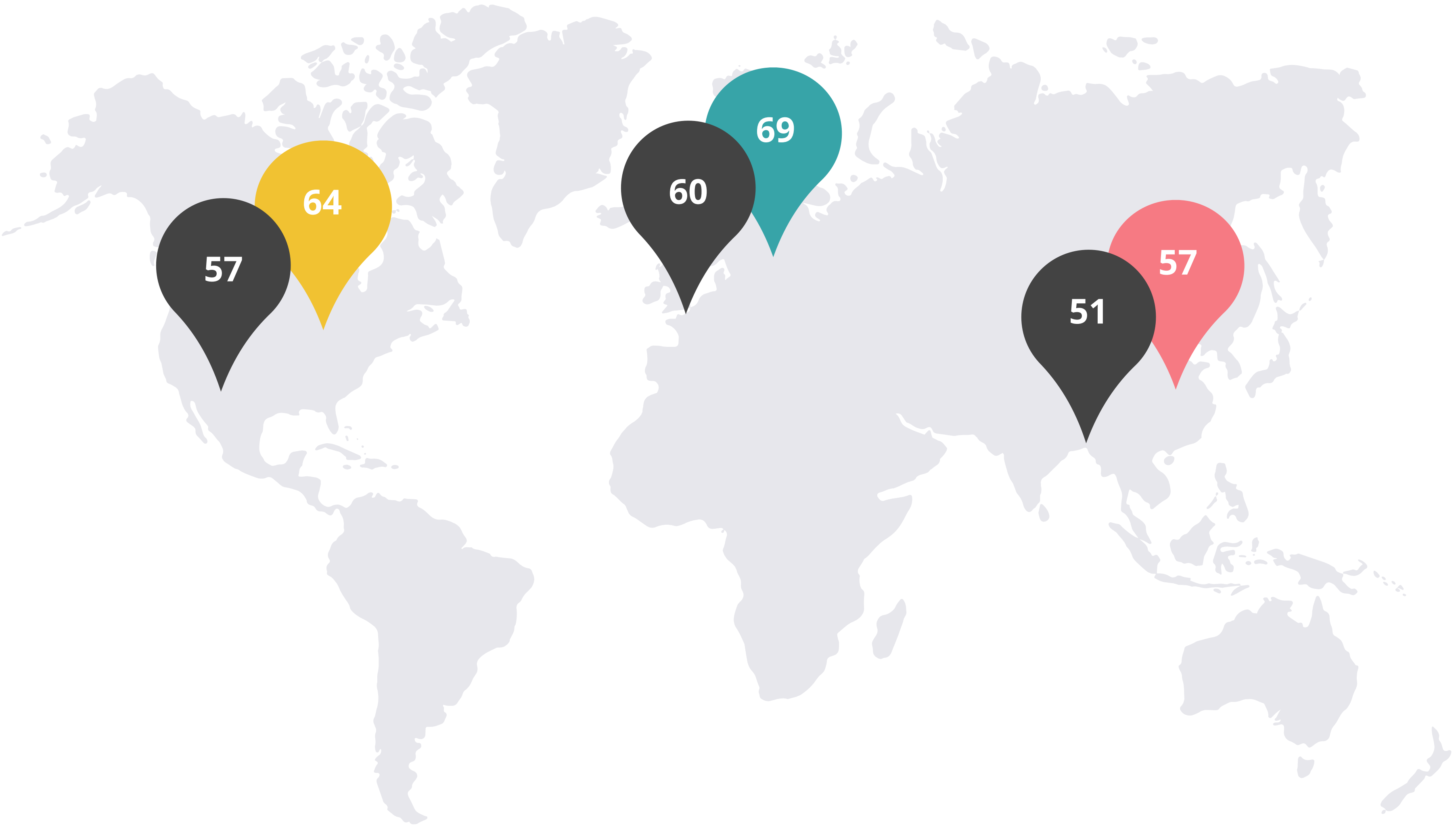


People who opened the emails performed better on **EVERY behavior** than those who didn't open the emails.

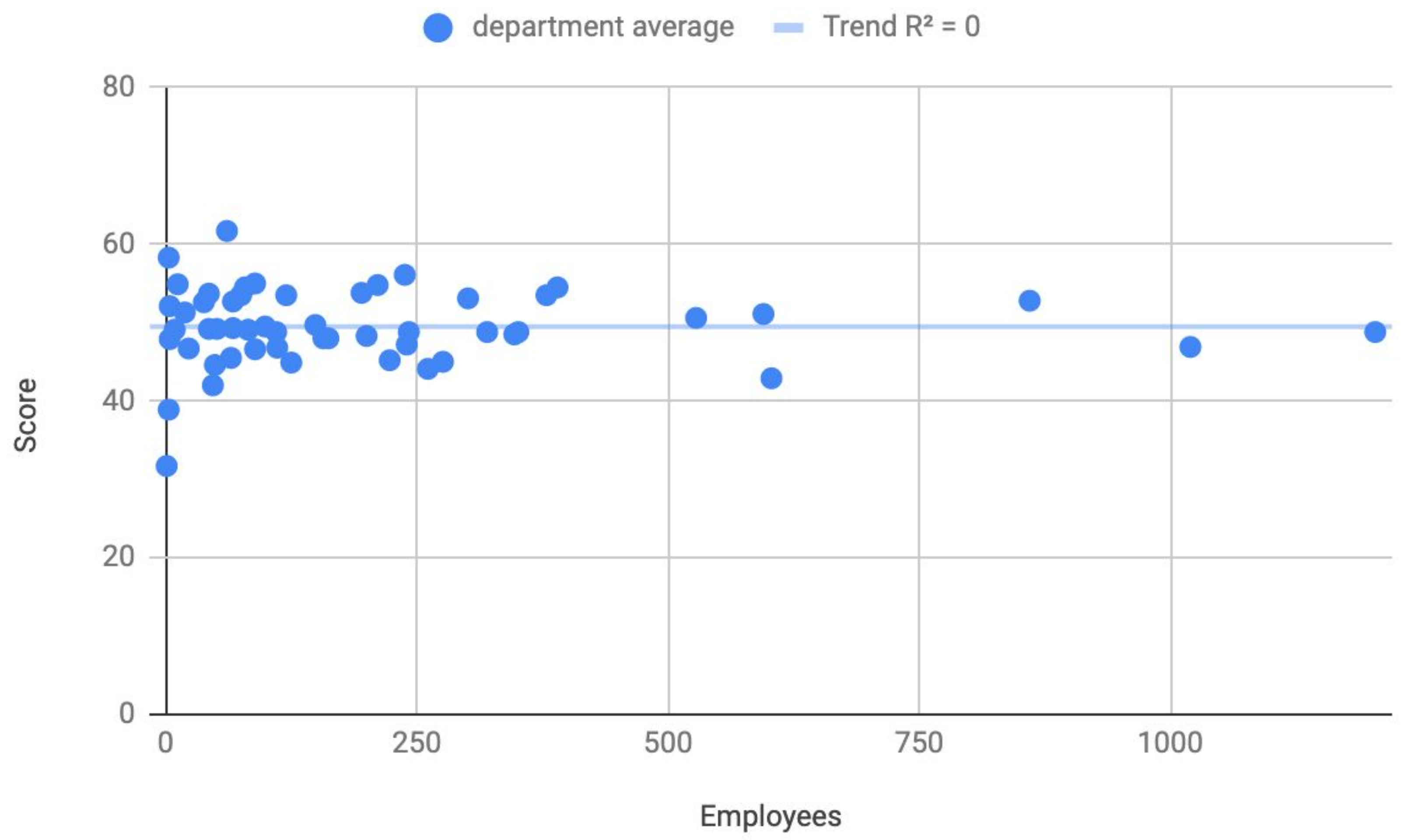
POP QUIZ TIME!

WHICH GEOGRAPHY IS THE LOWEST?

IT DOES



ARE BIGGER TEAMS MORE LIKELY TO MAKE SECURITY MISTAKES?

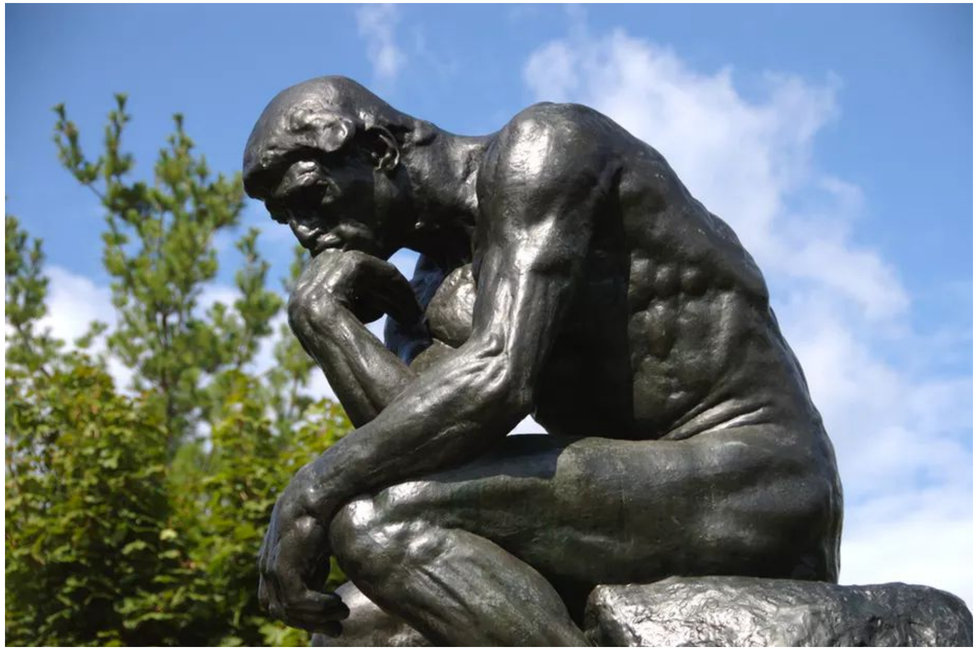


NOPE!

Team size had no correlation to the security score.

These results stayed true across all 3 snapshots.

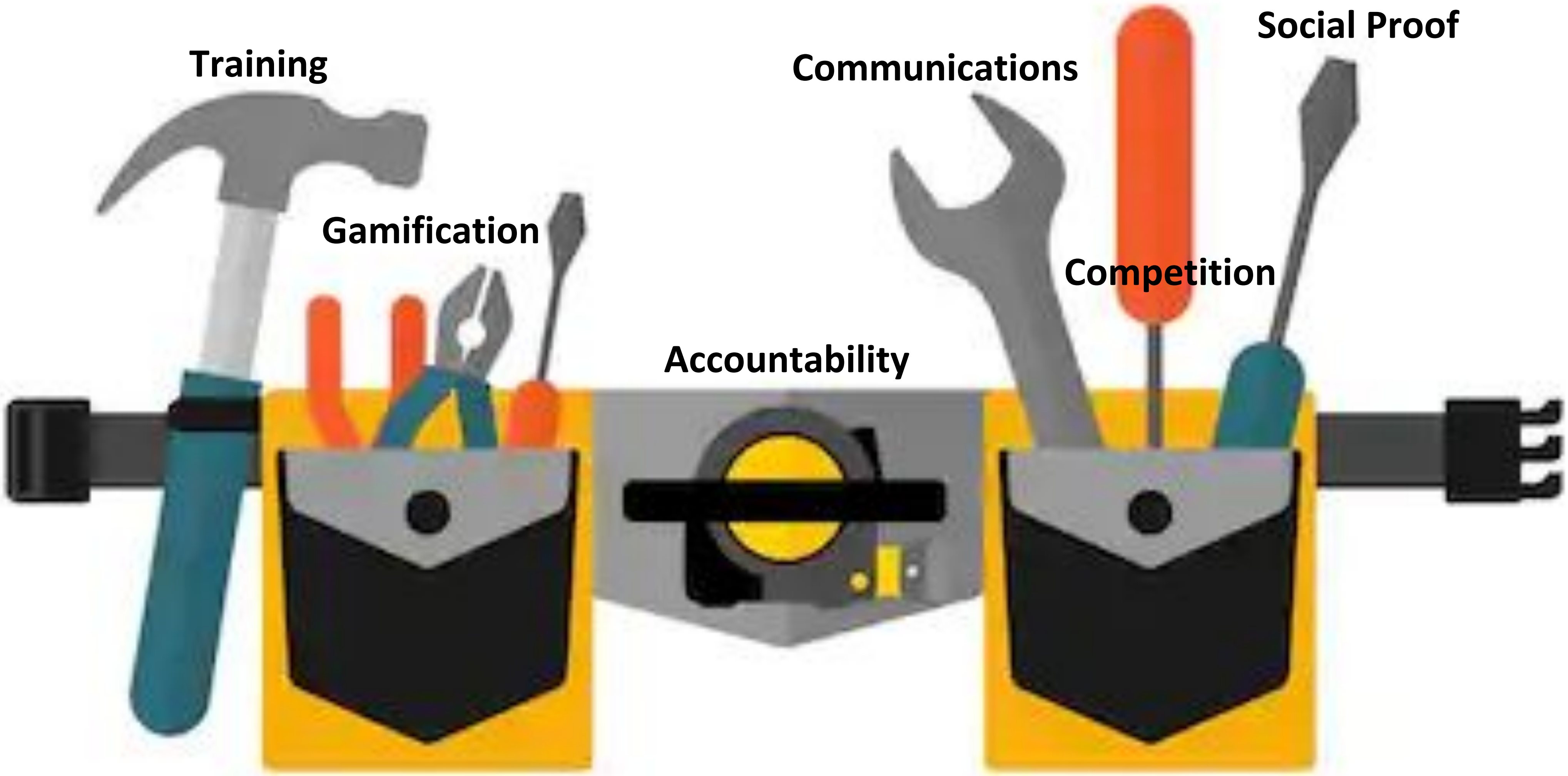
LESSONS LEARNED:
USE DATA TO DRIVE YOUR PROGRAM



What we *think* we know about how employees behave in our organizations might be wrong.

Without a data-driven approach to your awareness programs, you might be solving a problem that isn't there, or missing your biggest opportunity.

LESSON LEARNED:
MORE TRAINING ISN'T ALWAYS THE ANSWER



TRY THIS AT WORK!

1. **Find your top 3 behaviors**
2. **Find the data sources for them**
    a. Partner with other members of the security team
    b. Start small and expand
3. **Do trend analysis**
4. **Find culturally engaging ways of communicating findings**
    a. Leaderboards, Intranet sites, Emails, Slack
5. **Reward top behavior and focus on the bottom**

THANK YOU!

Aika.sengirbayeva@airbnb.com
Masha@elevatesecurity.com

APPENDIX

What we are working on next

Department comparisons across the company

What are the most highly correlated behaviors and indicators.

Replacing annual security with “behavioral mastery”