Know How Data Can Shape Security Engagement

Aika Sengirbay
Security Awareness Program Manager
Airbnb
<table>
<thead>
<tr>
<th>ABOUT AIKA SENGIRBAYEVA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trained in Cyber Security</td>
</tr>
<tr>
<td>Background in Incident Response &amp; Red Team</td>
</tr>
<tr>
<td>Building Security Awareness Programs for General and Technical communities</td>
</tr>
<tr>
<td>Passionate about building security culture</td>
</tr>
</tbody>
</table>
TRANSFORM EVERY EMPLOYEE TO SECURITY SUPERHUMAN
PREVIOUS STATE

Compliance
Check the box security

Unquantified
Unmeasured, no improvements

One Size Fits All
Same training for everyone

No Replay-ability
Not dynamic, no personalization, heavy churn
IN RESULTS

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
THE INDIVIDUAL SECURITY SNAPSHOT

Flimsy    Tenuous    Sturdy    Fortified    Indestructible
THE 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
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
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
TOP SECURITY BEHAVIORS

- Phishing - compromised creds
- Reporting suspicious emails
- Password management adoption
- Training
STEP 3
FINDING THE DATA
DATASETS

Phishing
Reporting incidents & suspicious emails
Secrets & Passwords Management
Training completion
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
EDUCATION LEVELS (STATIC) VS. CREDIT SCORE (DYNAMIC)
SOCIAL PROOF

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.
You were 1.2x more likely to be compromised than people in your department.

Strengthen skills
LastPass Use

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

Autodesk CEO Andrew Anagnost uses LastPass too!

12% of your department has installed LastPass

Installed LastPass

Used LastPass
INTRINSIC MOTIVATION - ACHIEVEMENT

Your Achievements

- First Phishing Detection Pass
- First Phishing Reporting Pass
- Installed and Activated LastPass
- Completed All Trainings
Here's your SECURITY SNAPSHOT

Keep up the good work!

Here's your SECURITY SNAPSHOT

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

Nice Work!

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

Eeeek!

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

![Score]

Review tests

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.

![Score]
COMPROMISED

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

REPORTED

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

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!

REPORTED

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

15.6% of your department has installed LastPass

You earned a badge!

LastPass Use

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

Autodesk CEO Andrew Anagnost uses LastPass. You should too!

15.6% of your department has installed LastPass

Install 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

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

Sign up for Trainings

Annual Security Training

Green Belt Developer Training
SHOWCASE OF THE IMPACT
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 “
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 training.

_512 hours saved_
YEAH THAT’S COOL,

BUT DID IT WORK..?
**Behaviors Improved**

- **Compromised**: 83%
- **Reporting**: 32%
- **Passwords Manager Adoption**: 87%
- **Training Completion**: 7%
170% increase in top performers

31% decrease in low performers

It is harder to motivate low performers to change than it is to get medium performers become high performers.
Low performers aren’t good at opening security emails and doing the desired security behaviors.
LESSONS LEARNED
INTERNAL STAKEHOLDER BUY-IN

CSO/CISO

Security Team

Legal

Human Resources

Teams with Datasets
RUN A PILOT
TAKEAWAYS

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 (in spreadsheets)
4. Know your metrics
5. Find culturally engaging ways of communicating findings
   a. Leaderboards, Intranet sites, Emails
THANK YOU!

aika.sengirbayeva@airbnb.com