“Should I Worry?”

A Cross-Cultural Examination of Account Security Incident Response

Elissa M. Redmiles

@eredmil1

eredmiles@cs.umd.edu

NSF Graduate Research Fellowship Program

University of Maryland 1856

MARYLAND CYBERSECURITY CENTER

facebook

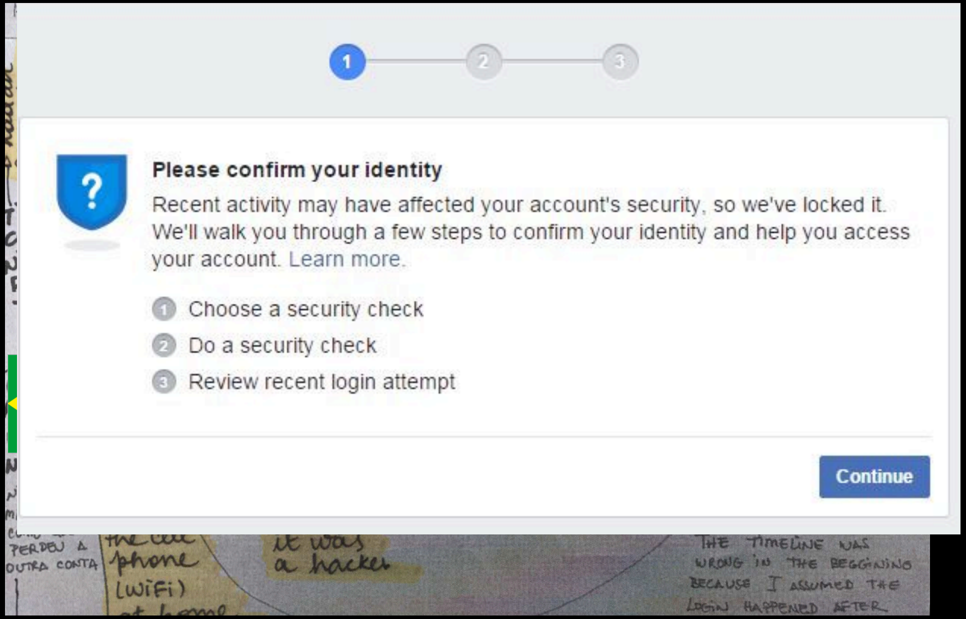
How do users respond when their accounts are attacked?

Cross cultural interview study of users' process of incident response (n=67)

Investigate users' process of incident response within 14 days after a suspicious login incident to their real Facebook account

Participants construct causal timelines of the incident and pre- / post-behavior

Interviewed 67 participants from five countries



Please confirm your identity

Recent activity may have affected your account's security, so we've locked it. We'll walk you through a few steps to confirm your identity and help you access your account. Learn more.

1. Choose a security check
2. Do a security check
3. Review recent login attempt

Continue
PERDEU A
OUTRA CONTA
phone
(WiFi)
it was
a hacker
THE TIMELINE WAS WRONG IN THE BEGGINING BECAUSE I ASSUMED THE LOGIN HAPPENED AFTER

Carefully designed methodology to ensure validity

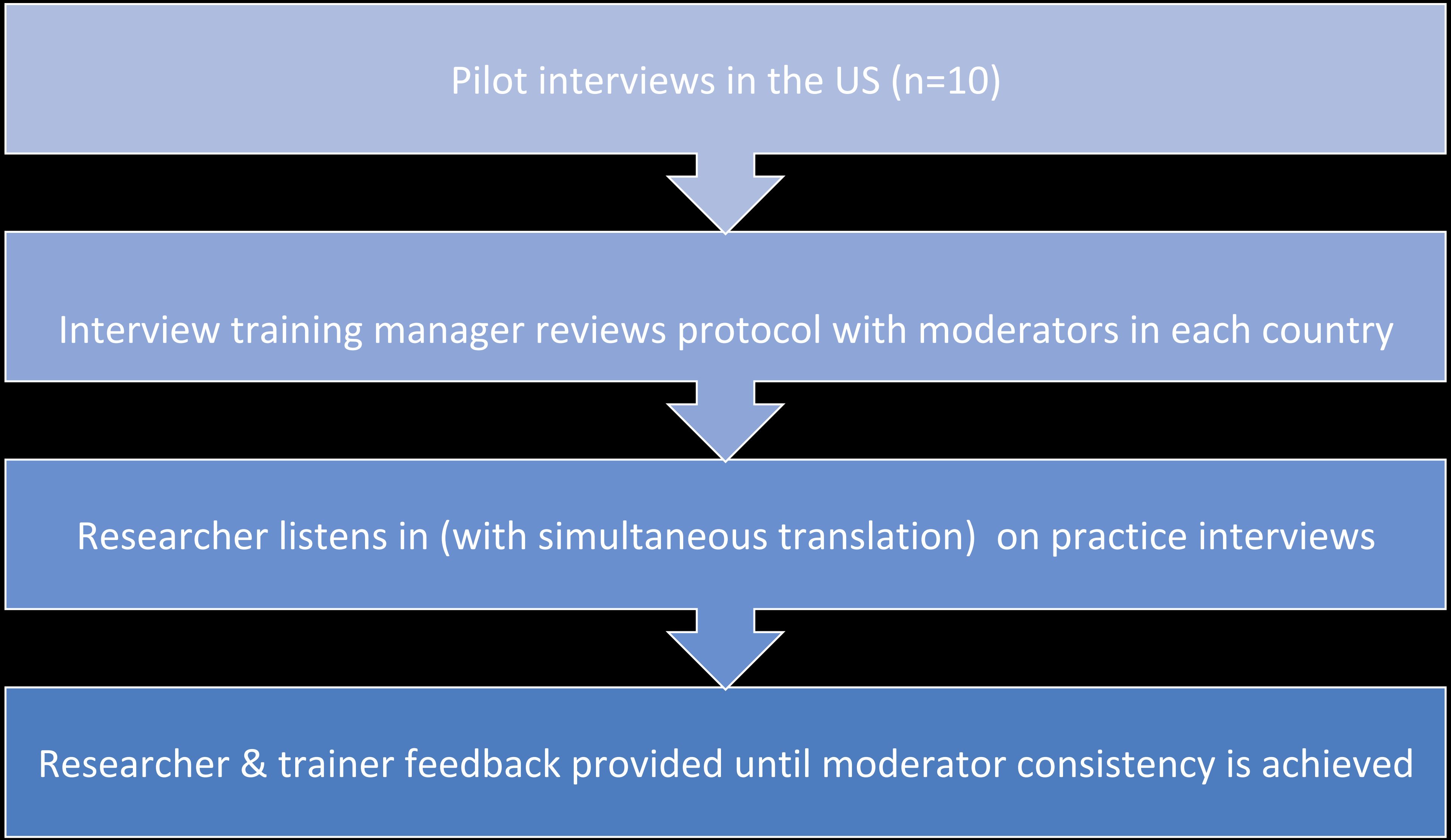
Step 1 Use facebook log data to identify users from the 5 selected countries who had a suspicious login incident

Step 2 Email eligible users to invite for a 30 minute native language in-person interview within 14 days of incident

Step 3 Aim for 15 participants per country, diversify on gender, age & education

Step 4 Validate behavioral reports for on-Facebook behaviors against log data (91% accuracy for user reports)

Extensive training to ensure cross-country validity



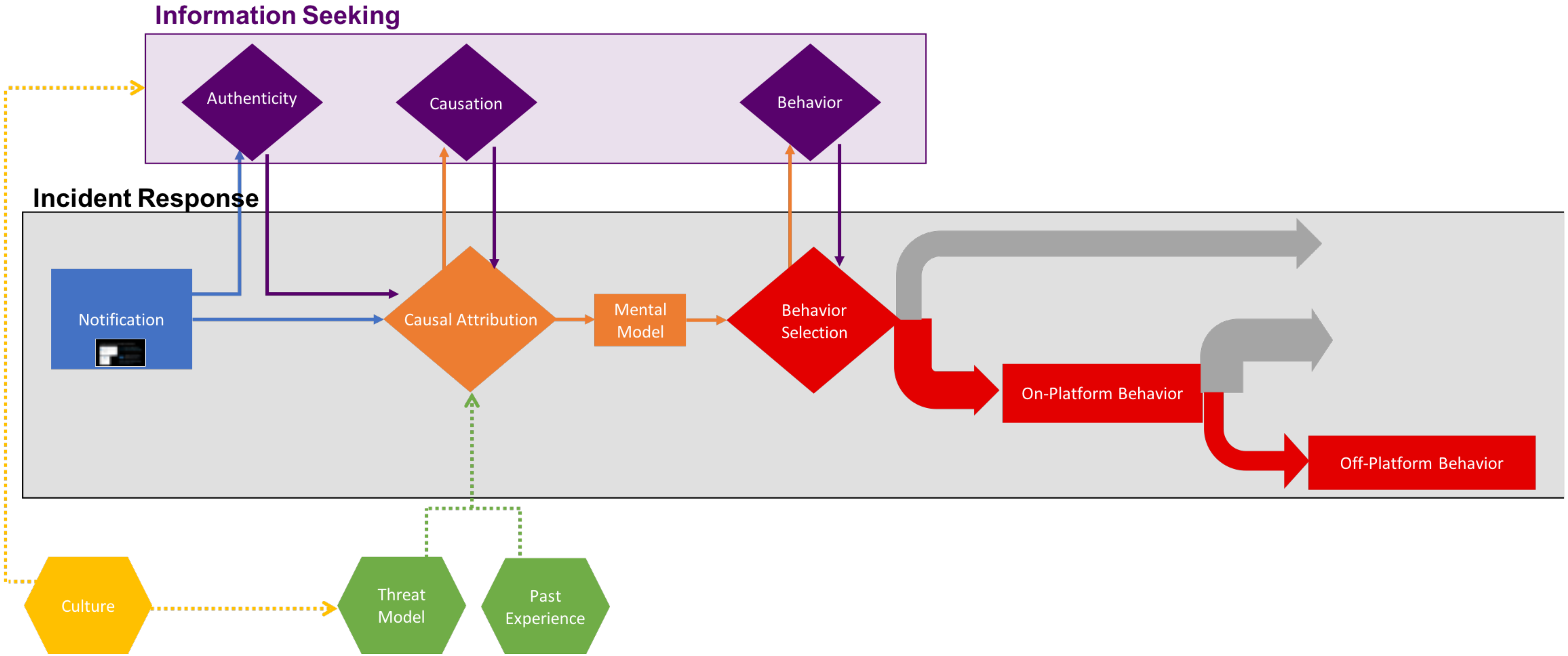
Pilot interviews in the US (n=10)

Interview training manager reviews protocol with moderators in each country

Researcher listens in (with simultaneous translation) on practice interviews

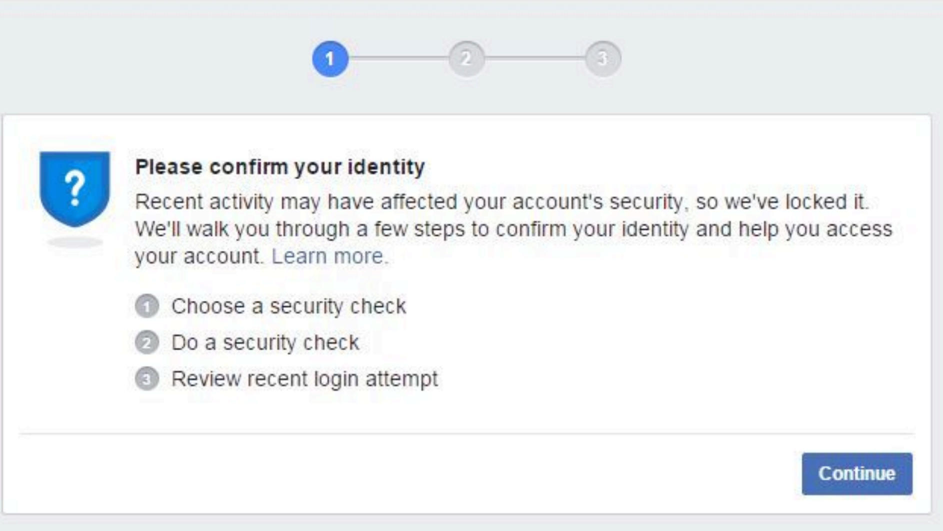
Researcher & trainer feedback provided until moderator consistency is achieved

Common process of account security incident response across participants from five countries



Elissa M. Redmiles

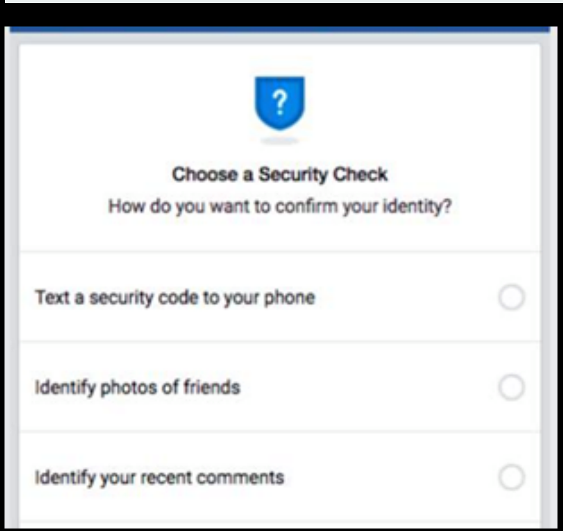
Incident awareness through notification



Please confirm your identity

Recent activity may have affected your account's security, so we've locked it. We'll walk you through a few steps to confirm your identity and help you access your account. Learn more.

1. Choose a security check
2. Do a security check
3. Review recent login attempt



Choose a Security Check

How do you want to confirm your identity?

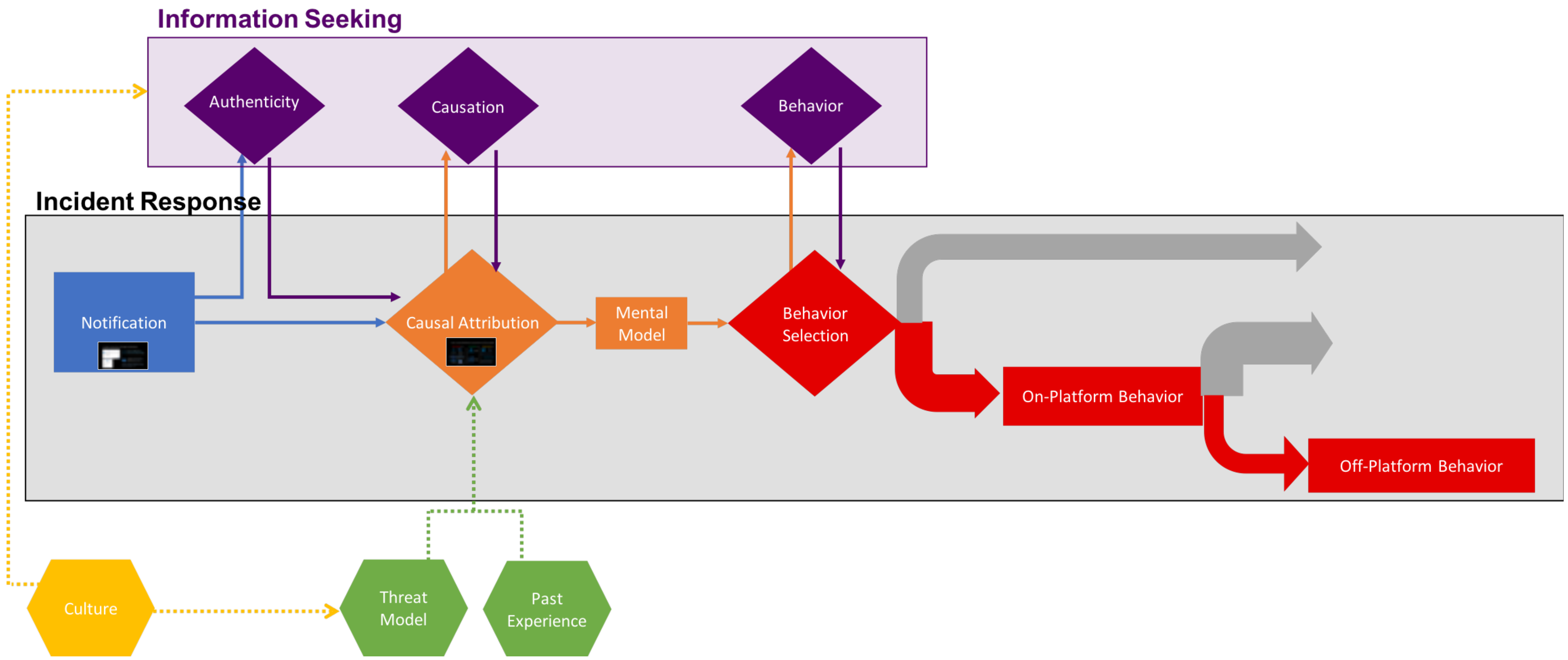
- Text a security code to your phone ○
- Identify photos of friends ○
- Identify your recent comments ○

Awareness is triggered by the unique authentication process rather than the notification message

Secondary authentication task created a sense of partnership between platform and user

“it made me feel like...[Facebook] is on top of the game...somebody is watching out to make sure I don’t get hacked” --DE1

Common process of account security incident response across participants from five countries



Elissa M. Redmiles

Users’ causal attributions (classifications) of the incident

False Positive (n=29)

New location

Unsafe or “bad” behavior

“I hacked likes. So basically, I just hacked number of likes on the post” VN1

Mistyped password

New or rarely used device

VPN/private browsing

True Positive (n=31)

Unknown attacker

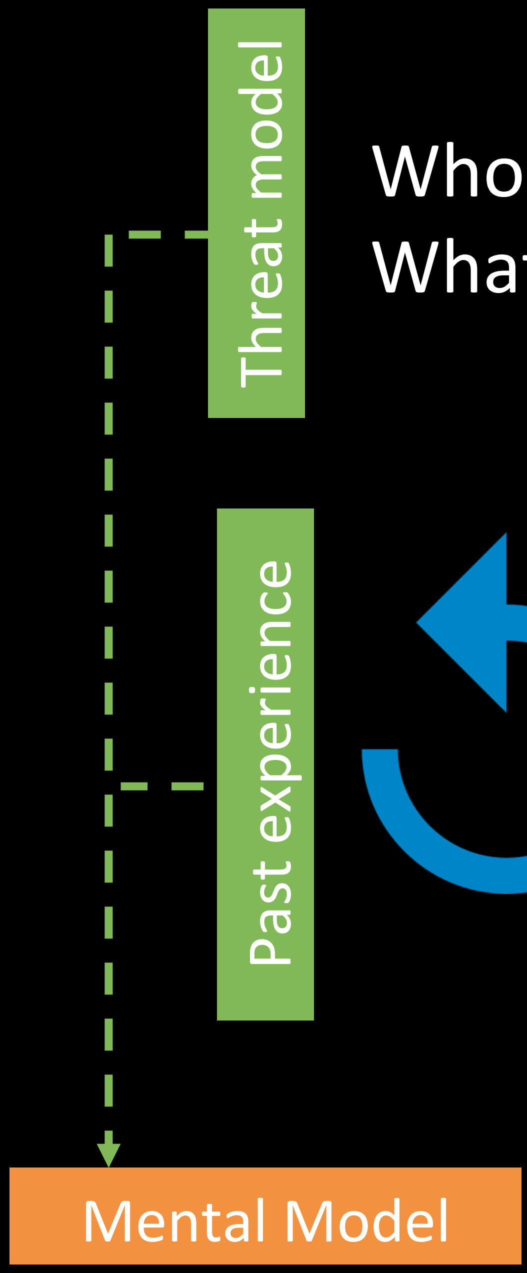
Known attacker

Random Check (n=7)

“a random security check, like TSA does at the airport” US2

“like a checkup to make sure [the] account was ok” BR7

“I hear about fake news a lot...I think they are cracking down… everyone had to do this” IN4

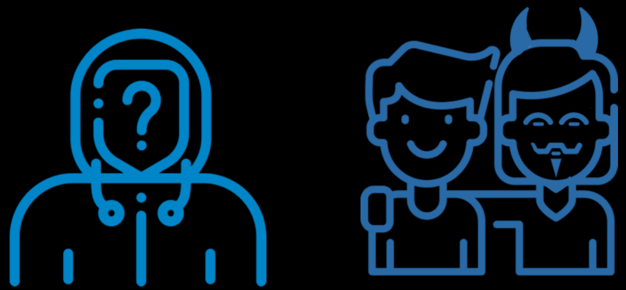


Who?

What?

facebook

threat model



Wash “digital graffiti artist”

Wash “burglar”

the Spy

the Snoop

the Who Else

the Humiliator

New!

“The first time that it appeared, I thought it was someone who was trying to access to my Facebook but the next times, I realized that it was just Facebook [trying] to enhance the security [again]” VN6

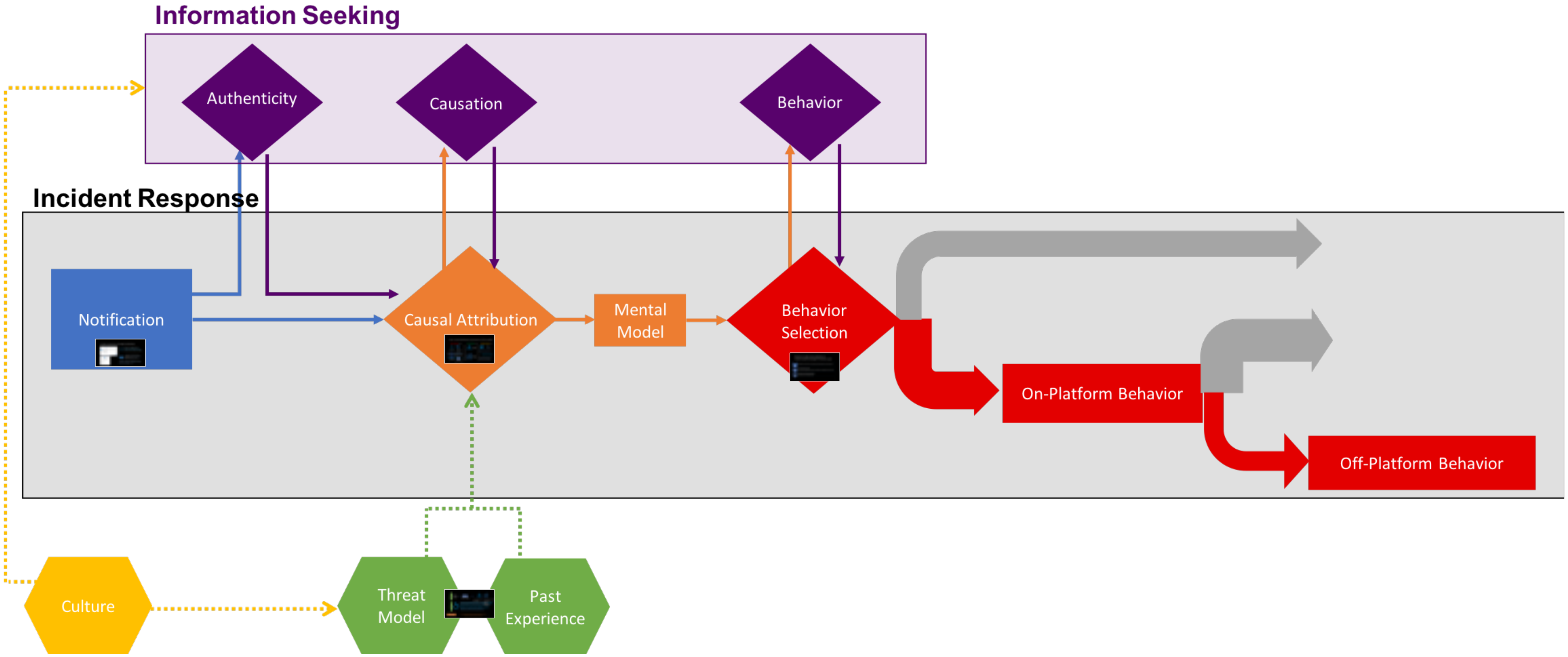
Prior experiences that altered mental models were only prior Facebook experiences, not generalized from other platforms

Repeated prior FN made participants disregard the current incident, even though the platform identified it as higher risk

“the first time, I was worried…[now I understand] Facebook asks all users this when they go into a foreign country [now] I don’t think it has to do with me” DE2

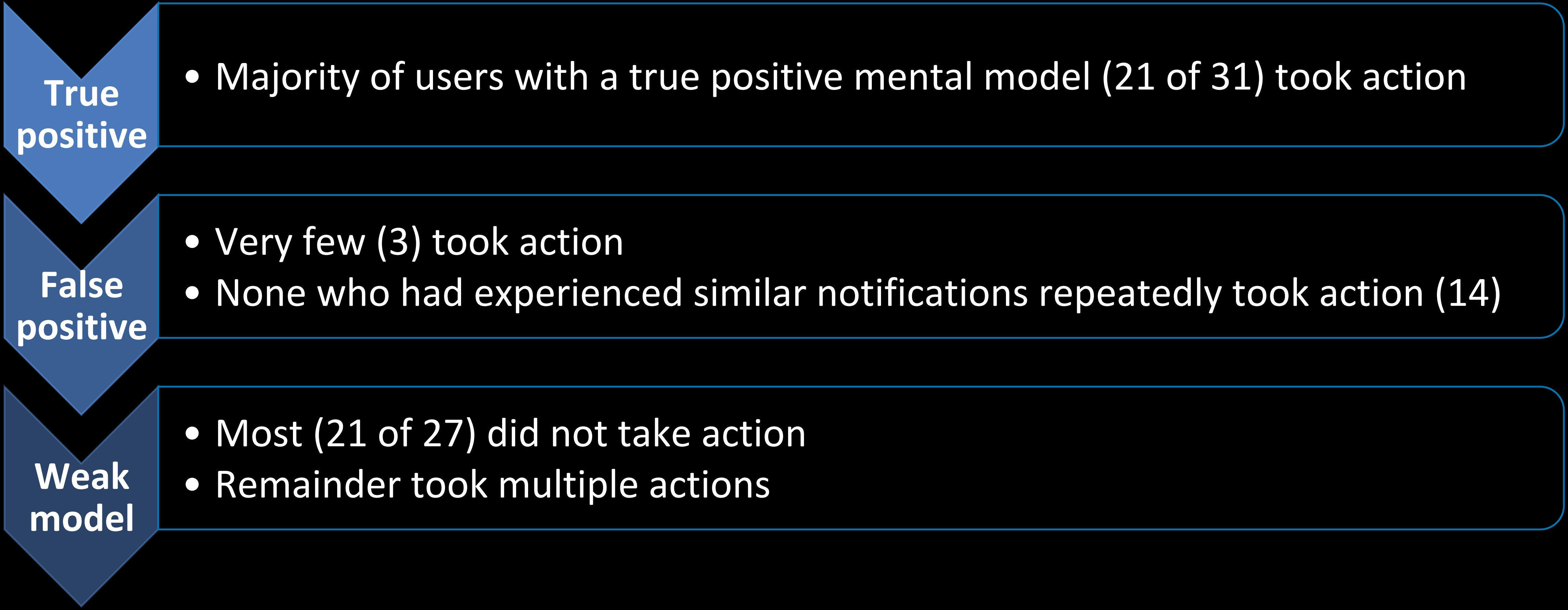
Of participants with plausible mental models (n=51) over half of those mental models were weak

Common process of account security incident response across participants from five countries



Elissa M. Redmiles

Decision to take action depends on mental model & strength of mental model



True positive

- Majority of users with a true positive mental model (21 of 31) took action

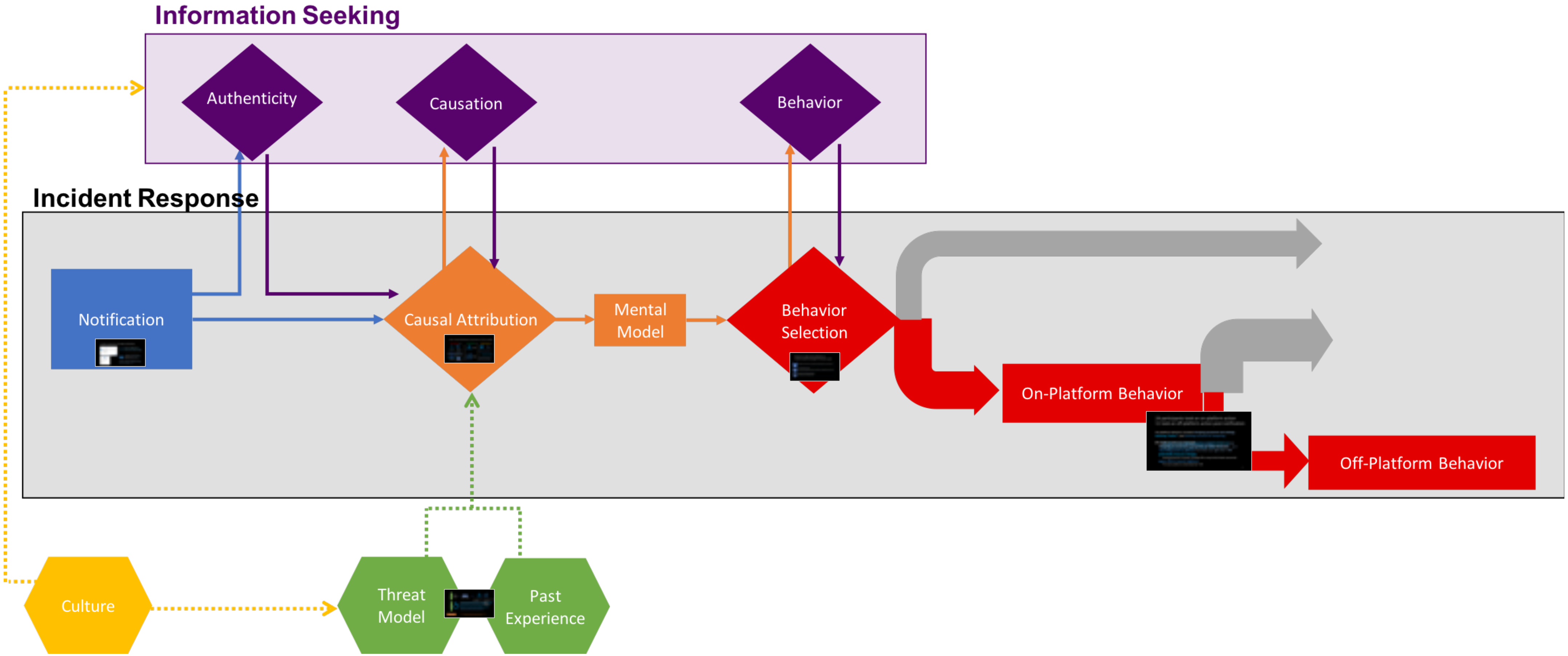
False positive

- Very few (3) took action
- None who had experienced similar notifications repeatedly took action (14)

Weak model

- Most (21 of 27) did not take action
- Remainder took multiple actions

Common process of account security incident response across participants from five countries



Elissa M. Redmiles

24 participants took an on-platform action 11 took an off-platform action post-notification

On-platform behavior included **changing passwords and settings**, **behaving “better”**, and **checking accounts for tampering**

“I checked the messages to see if there was anything [sent] deceiving other friends” IN3

[illegible] changes in my friend list and [illegible]” IN2

[illegible] receive [illegible] account...so it won’t be a surprise and I can kick them out right then” BR4

Off-platform behavior included

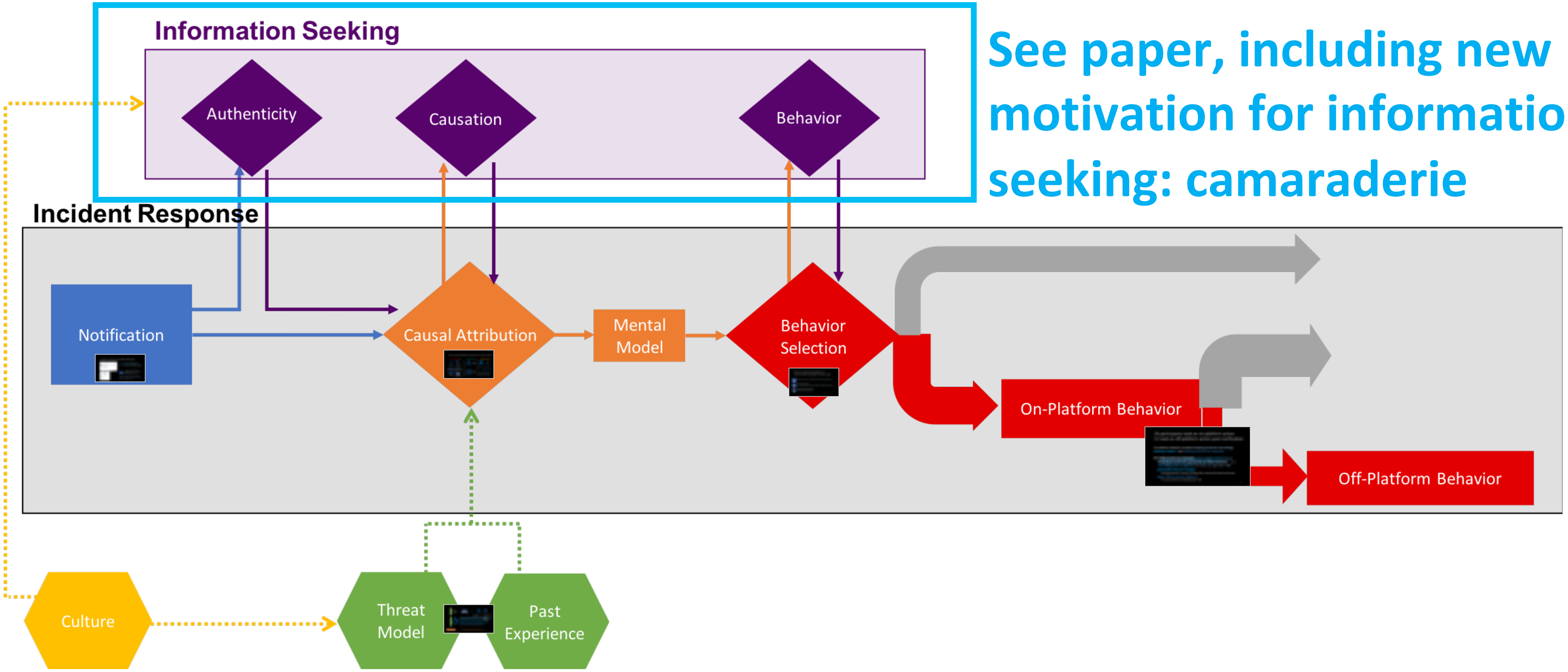
- **changing to novel new passwords on other accounts**
- **improving security posture**
- **potentially insecure changes**

    (saving passwords in browser, avoiding VPN, using similar/simpler passwords)

- **vague efforts toward vigilance**

    “I’m more careful on email [now] too” US5

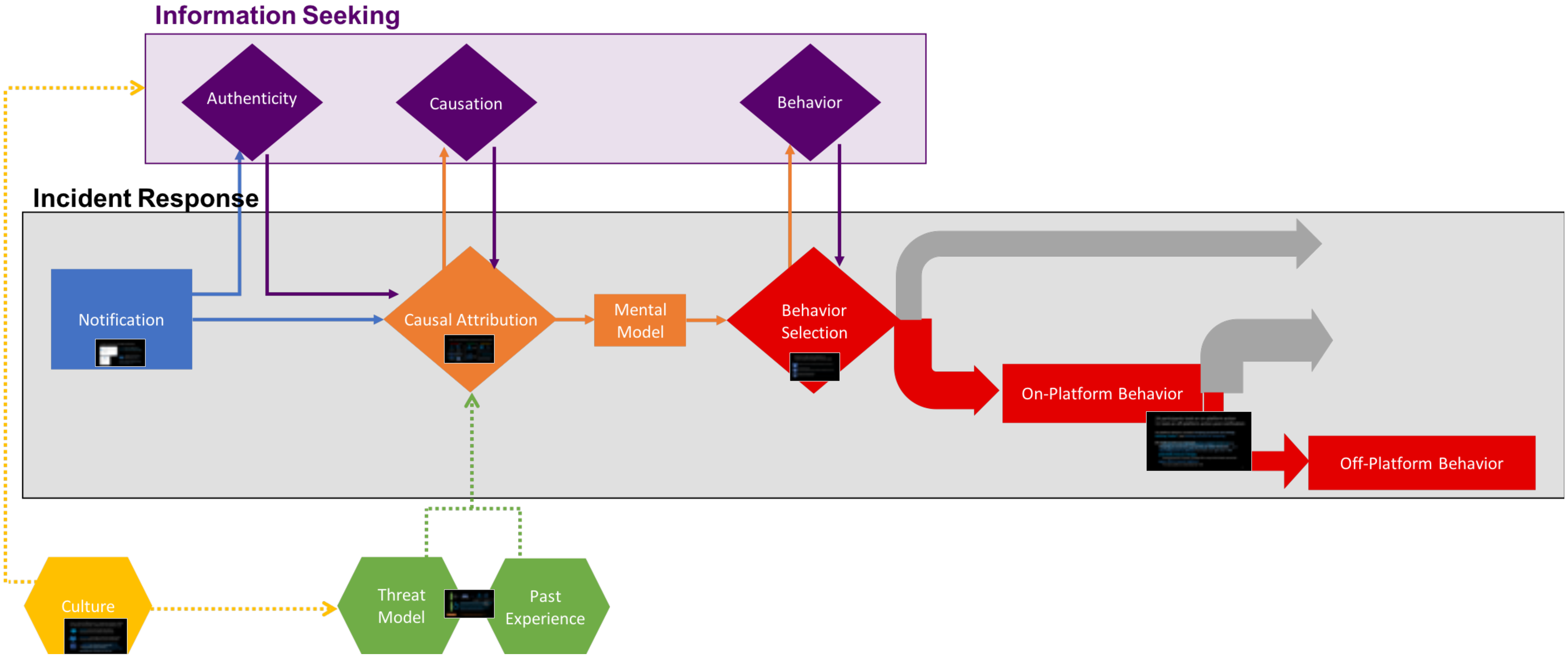
Common process of account security incident response across participants from five countries



See paper, including new motivation for information seeking: camaraderie

Elissa M. Redmiles

Common process of account security incident response across participants from five countries



Elissa M. Redmiles

Cross-cultural differences in response process relate to internet censorship, collectivism & platform use

Censored country threat models (VN, IN) focus toward government-surveillance related threats

Collectivistic country (BR, VN, IN) threat models focused on known attackers & different sources of information

Facebook use (e.g., business vs. passive) also influenced threat models & defenses

"I would feel that someone was violating me. And I wouldn't know what to do because then I wouldn't be able to do anything to recover." BR13

Interesting note: skill did not come up!

Improving the incident response process

Weak mental models make it unlikely users will take action

Causal modeling by platform could help augment user models

Repeated false positives make it hard to regain user attention

For now: indicate classifier confidence transparency

Future: create user <> classifier feedback mechanisms

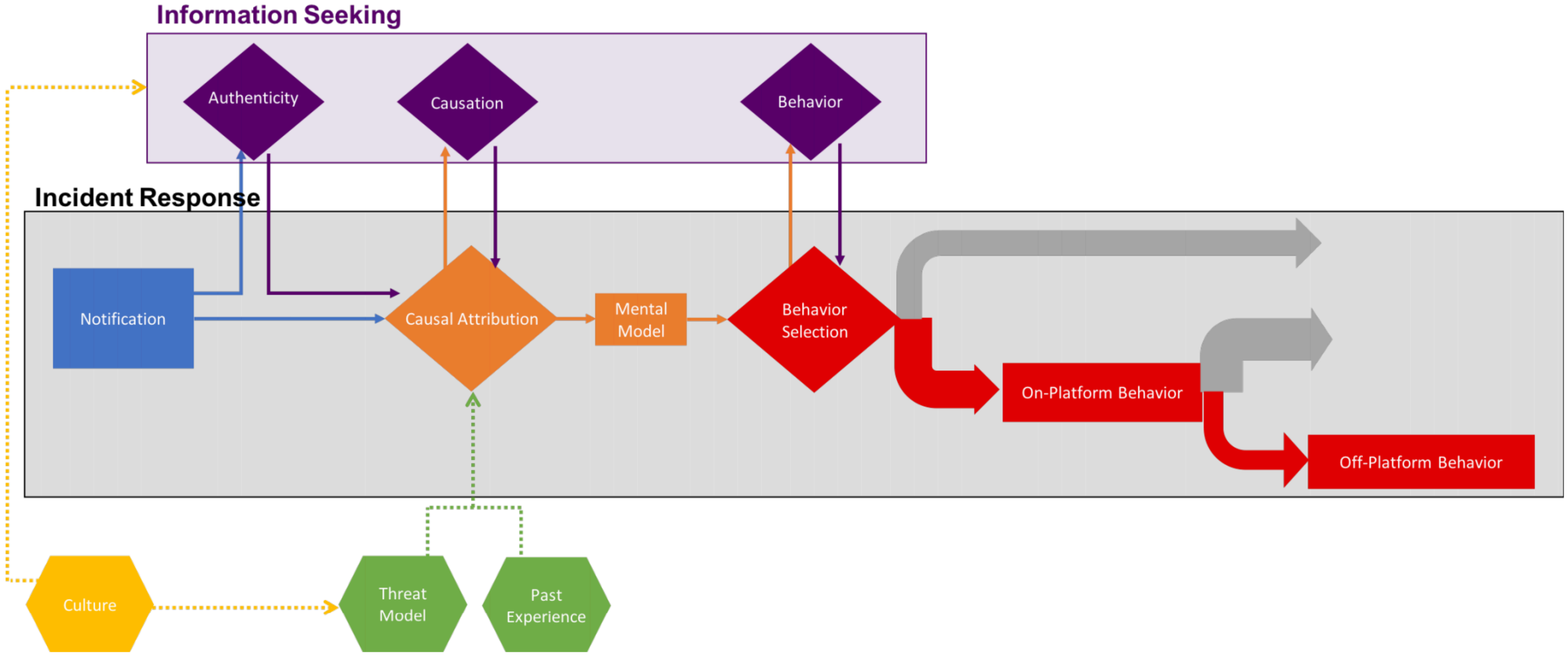
Develop better defenses for known attacker threat models

Key issue for non-Western cultures & domestic violence victims

“Should I Worry?” A Cross-Cultural Examination of Account Security Incident Response

Elissa M. Redmiles

Questions? eredmiles@cs.umd.edu



Brazil

Germany

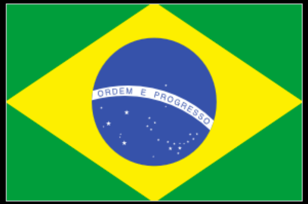
India

USA

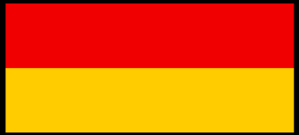
Vietnam

Backup

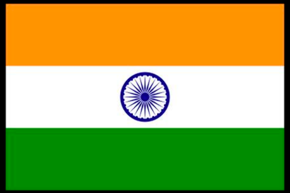
Participant Demographics



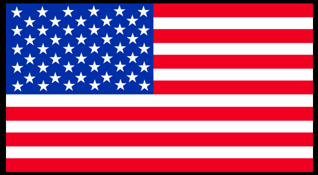
15 participants



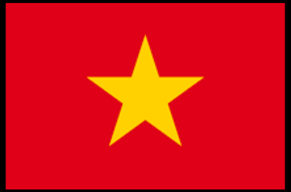
11 participants



15 participants



9 participants



17 participants

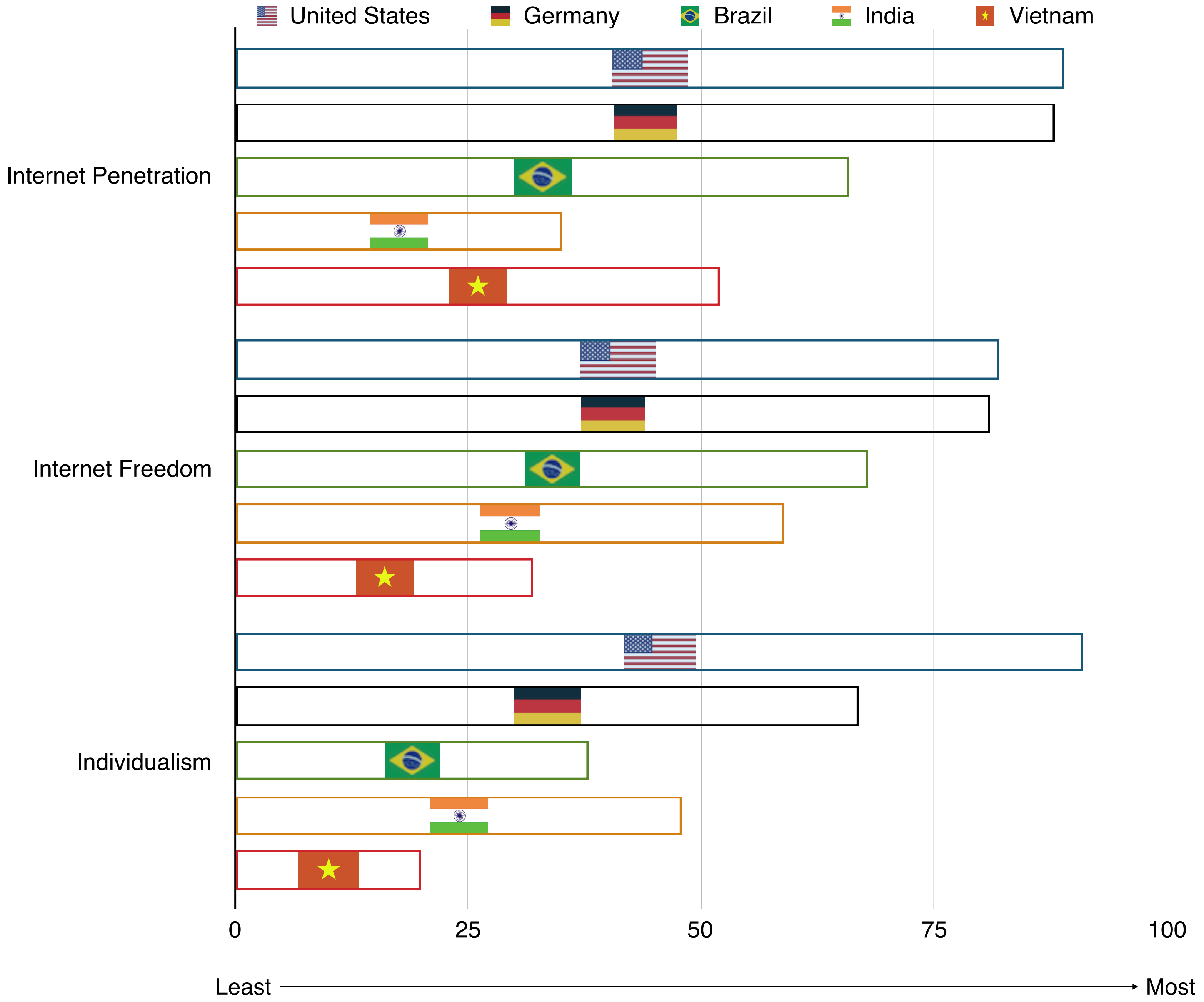
21% use for business

40% use messenger

68% male
IN & VN majority male

48% HS or below
IN all college+
Good balance elsewhere

68% millennials
VN, BR, IN very young
DE, US middle aged

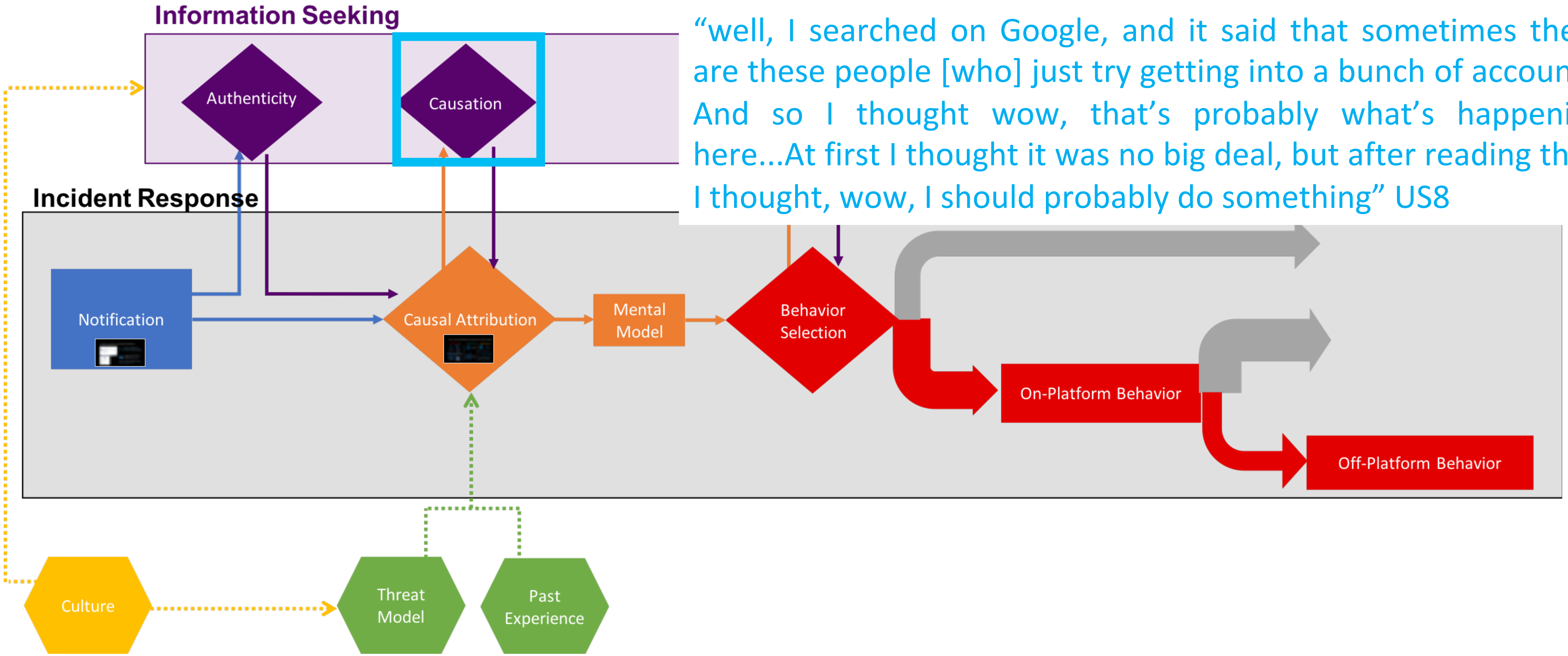

United States
Germany
Brazil
India
Vietnam
Internet Penetration
Internet Freedom
Individualism
0
25
50
75
100
Least
Most

Prior work has asked this question in reflective or hypothetical ways

Asking questions about incidents long in the past can lead to **telescoping** bias

Asking questions about hypothetical breaches raises issues of **ecological validity**

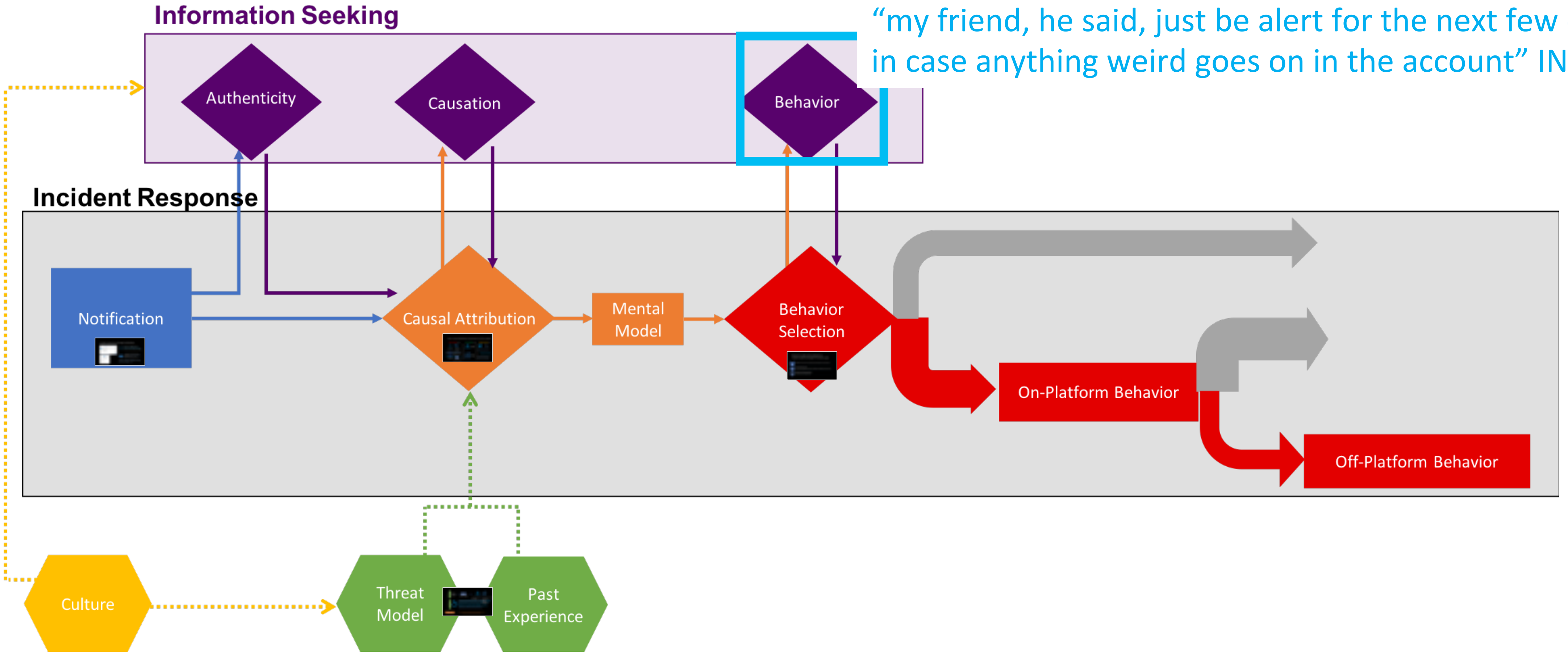
Common process of account security incident response across participants from five countries



"well, I searched on Google, and it said that sometimes there are these people [who] just try getting into a bunch of accounts. And so I thought wow, that's probably what's happening here...At first I thought it was no big deal, but after reading that, I thought, wow, I should probably do something" US8

Elissa M. Redmiles

Common process of account security incident response across participants from five countries



“my friend, he said, just be alert for the next few days, in case anything weird goes on in the account” IN12