RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PART3-T01**

A Whole Lotta BS (Behavioral Science) about Cybersecurity

MODERATOR: **Lisa Plaggemier**
Executive Director, National Cybersecurity Alliance

PANELISTS:

Oz Alashe
CEO & Founder
CybSafe
@ozalashe

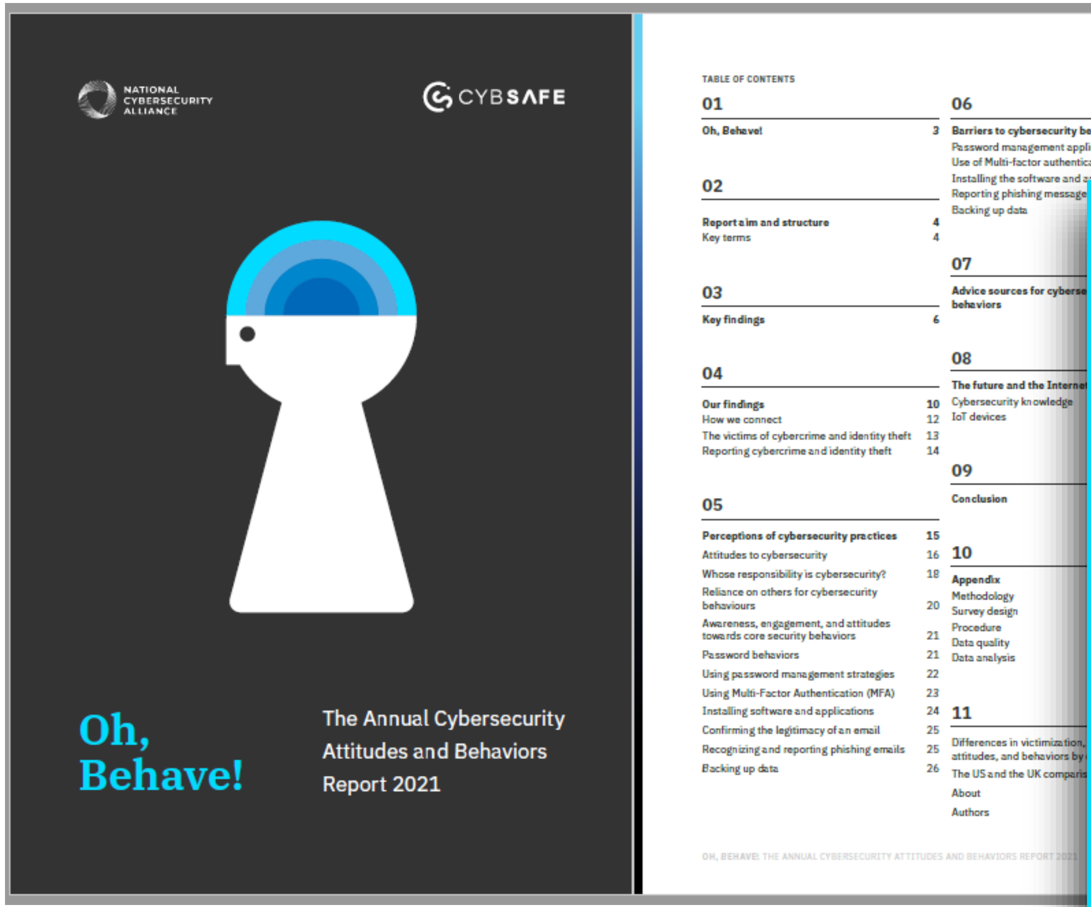
Dr. Deanna Caputo
Chief Scientist for Insider Threat Capabilities
Senior Principal Behavioral Psychologist
MITRE

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Oh, Behave!
The Annual Cybersecurity Attitudes and Behaviors Report 2021



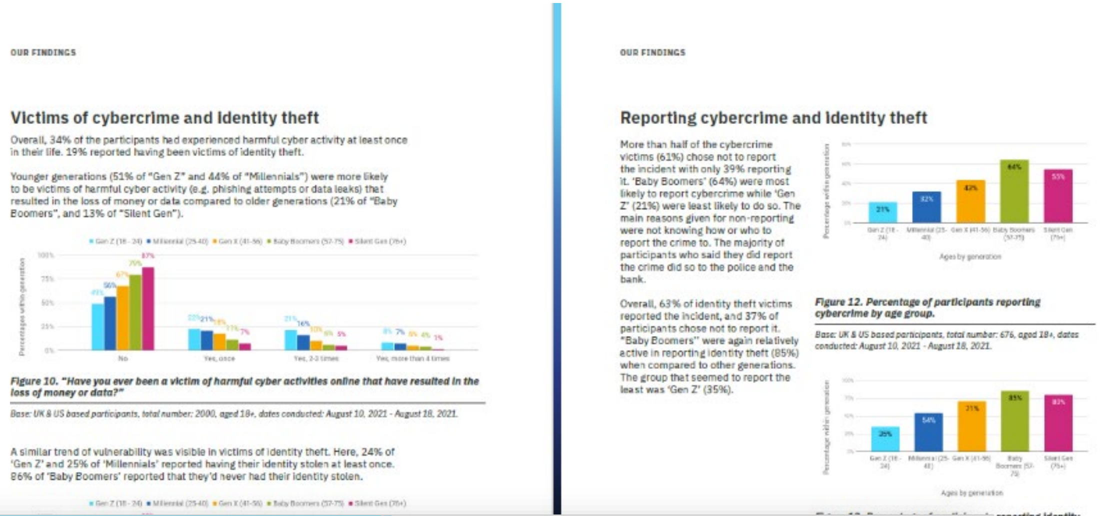
NATIONAL CYBERSECURITY ALLIANCE

CYBSAFE

Oh, Behave!

The Annual Cybersecurity Attitudes and Behaviors Report 2021

TABLE OF CONTENTS



Victims of cybercrime and identity theft

Overall, 34% of the participants had experienced harmful cyber activity at least once in their life. 19% reported having been victims of identity theft.

Younger generations (51% of "Gen Z" and 44% of "Millennials") were more likely to be victims of harmful cyber activity (e.g. phishing attempts or data leaks) that resulted in the loss of money or data compared to older generations (21% of "Baby Boomers", and 13% of "Silent Gen").

Figure 10. "Have you ever been a victim of harmful cyber activities online that have resulted in the loss of money or data?"

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

A similar trend of vulnerability was visible in victims of identity theft. Here, 24% of 'Gen Z' and 25% of 'Millennials' reported having their identity stolen at least once. 86% of 'Baby Boomers' reported that they'd never had their identity stolen.

Reporting cybercrime and identity theft

More than half of the cybercrime victims (61%) chose not to report the incident with only 39% reporting it. 'Baby Boomers' (64%) were most likely to report cybercrime while 'Gen Z' (21%) were least likely to do so. The main reasons given for non-reporting were not knowing how or who to report the crime to. The majority of participants who said they did report the crime did so to the police and the bank.

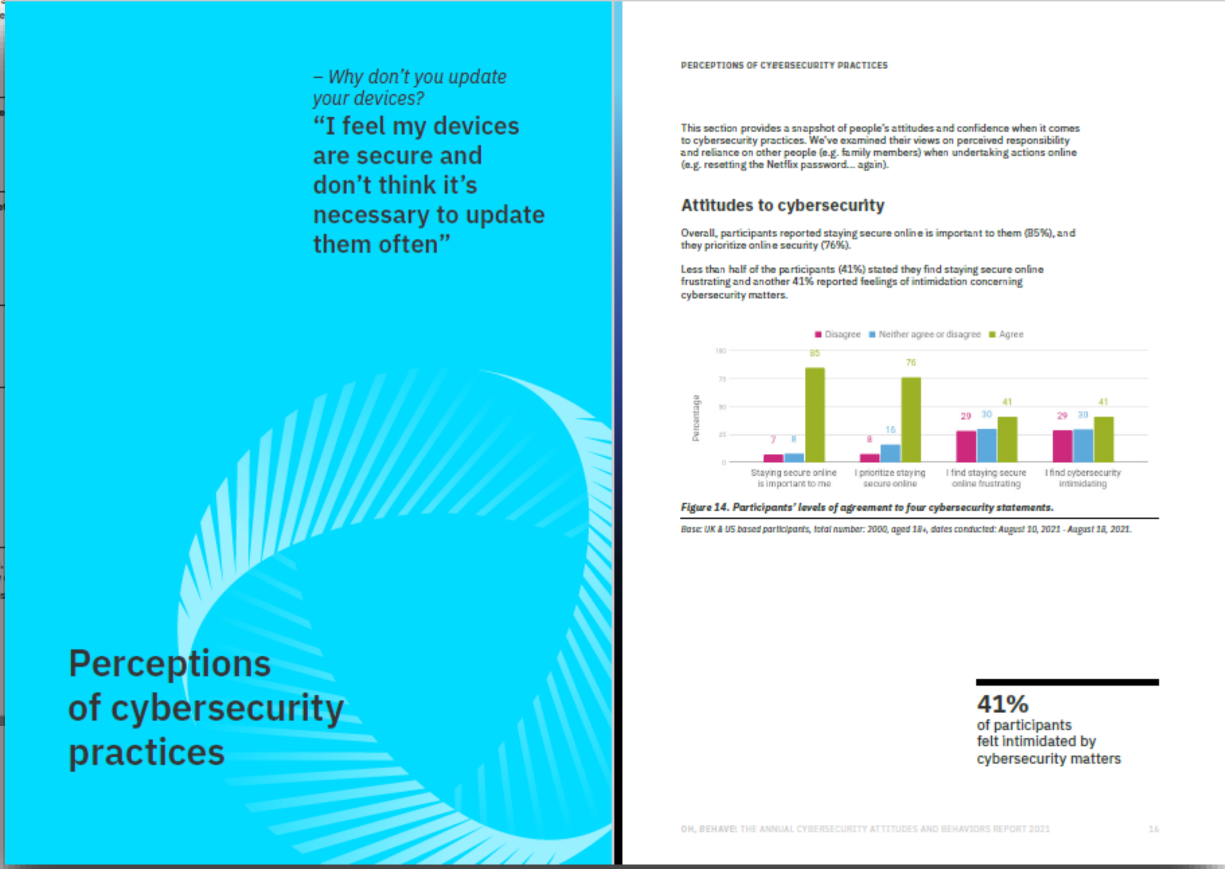
Overall, 63% of identity theft victims reported the incident, and 37% of participants chose not to report it. "Baby Boomers" were again relatively active in reporting identity theft (85%) when compared to other generations. The group that seemed to report the least was 'Gen Z' (35%).

Figure 12. Percentage of participants reporting cybercrime by age group.

Base: UK & US based participants, total number: 676, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

reporting identity

389, aged 18+, dates



– Why don't you update your devices?

"I feel my devices are secure and don't think it's necessary to update them often"

Perceptions of cybersecurity practices

This section provides a snapshot of people's attitudes and confidence when it comes to cybersecurity practices. We've examined their views on perceived responsibility and reliance on other people (e.g. family members) when undertaking actions online (e.g. resetting the Netflix password… again).

Attitudes to cybersecurity

Overall, participants reported staying secure online is important to them (85%), and they prioritize online security (76%).

Less than half of the participants (41%) stated they find staying secure online frustrating and another 41% reported feelings of intimidation concerning cybersecurity matters.

Disagree
Neither agree or disagree
Agree
Percentage
100
75
50
25
0
7
8
85
8
16
76
29
30
41
29
30
41
Staying secure online is important to me
I prioritize staying secure online
I find staying secure online frustrating
I find cybersecurity intimidating

Figure 14. Participants' levels of agreement to four cybersecurity statements.

Base: UK & US based participants, total number: 2000, aged 18+, dates conducted: August 10, 2021 - August 18, 2021.

41%
of participants felt intimidated by cybersecurity matters

1. What **motivates people to follow** security advice?

2. What are **the main barriers** when applying security advice in practice?

3. What can we learn that might help us better realise **desired behavior change**?

Our approach

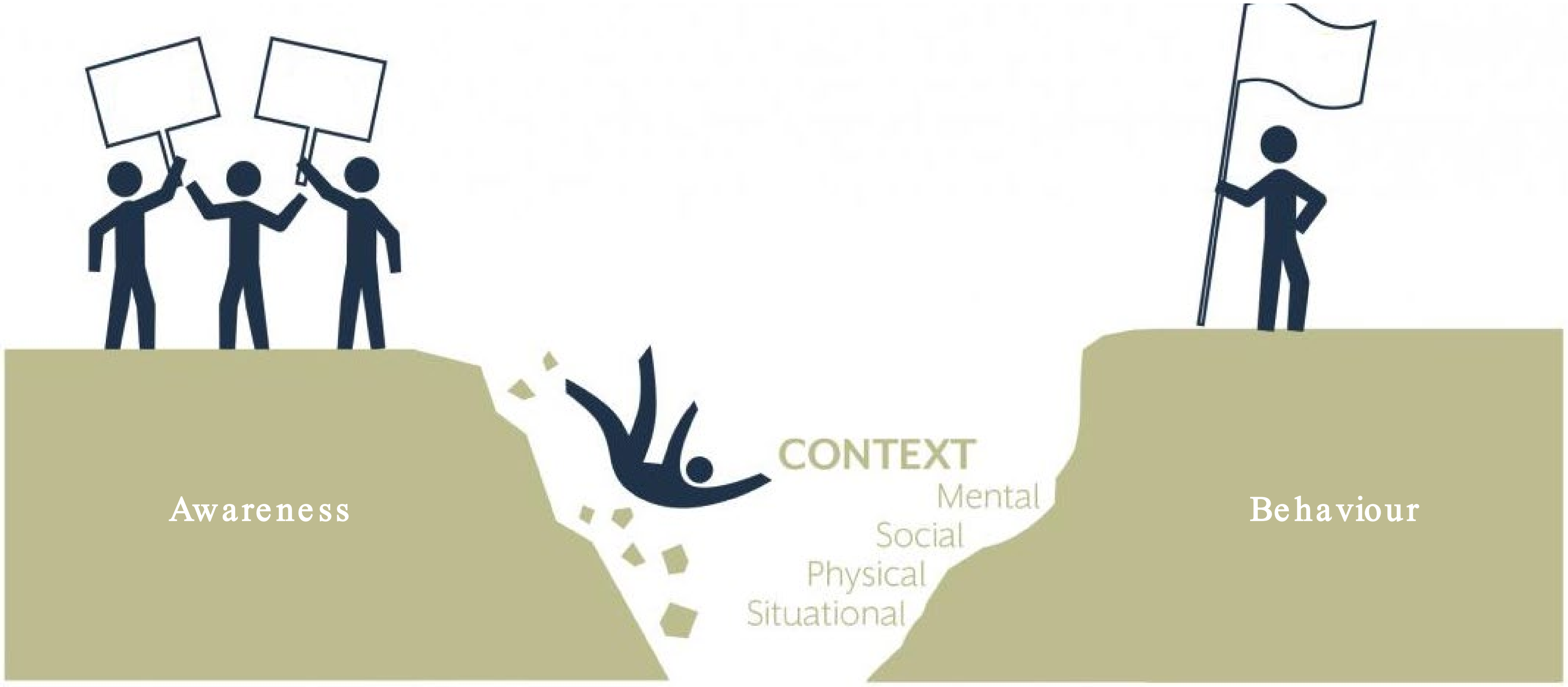
Security awareness, engagement, and attitudes towards good cybersecurity behaviours.

7 core security behaviours:

1. Creating strong and separate passwords
2. Using password management strategies
3. Using Multi-Factor Authentication (MFA)
4. Installing latest software/ applications
5. Checking messages legitimacy
6. Reporting phishing emails
7. Backing up data

(UK) NCSC Cyber Aware
(US) National Cybersecurity Alliance

Why


Awareness
CONTEXT
Mental
Social
Physical
Situational
Behaviour

Awareness

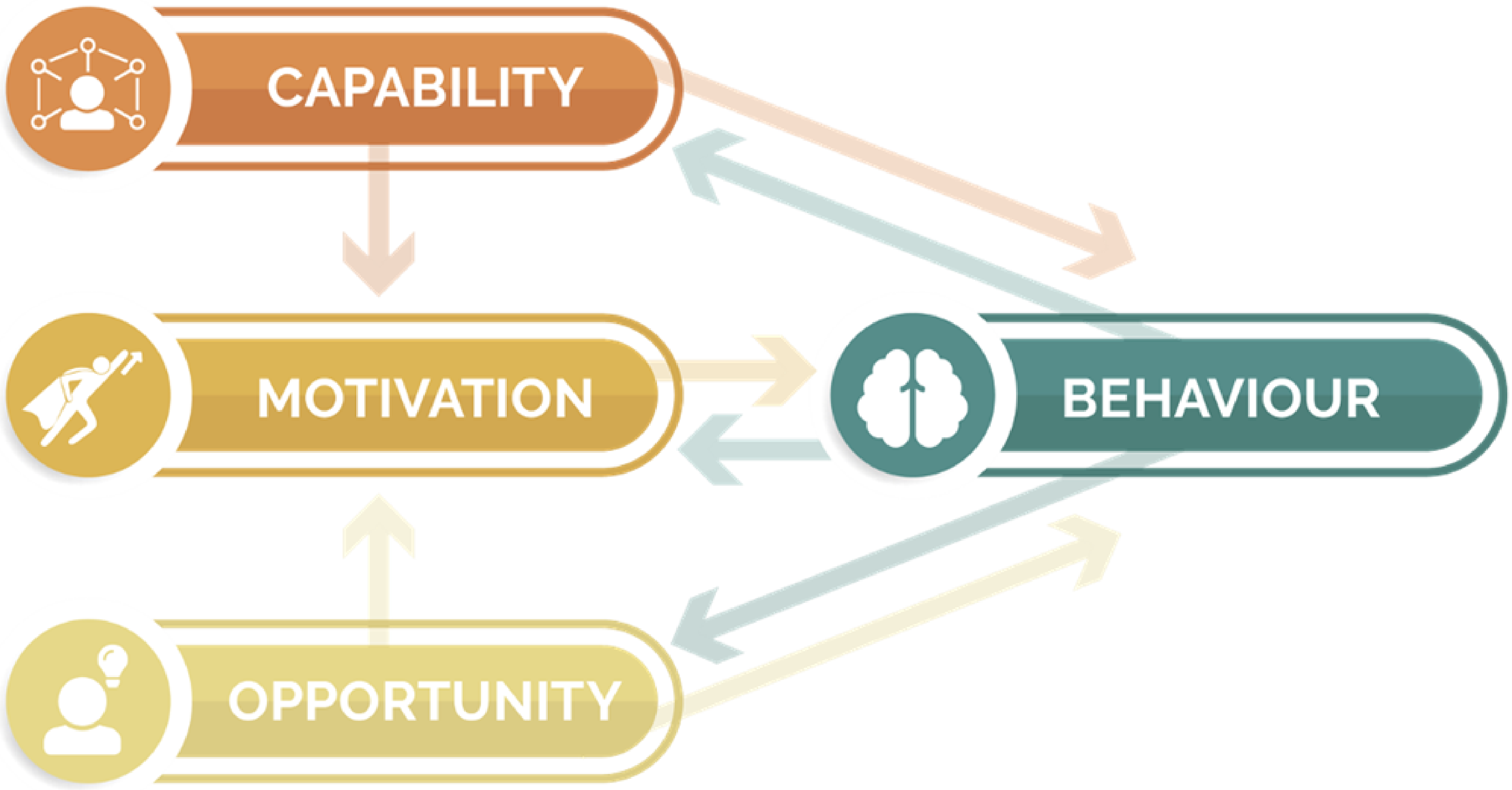
Physical & psychological ability

Decision Making

Conscious & unconscious

Environment

Physical & social



Our findings

NATIONAL CYBERSECURITY ALLIANCE

CYBSAFE

Oh, Behave!

The Annual Cybersecurity Attitudes and Behaviors Report 2021

34%

of the research survey participants reported **having experienced harmful cyber activity** at least once in their lives.

61%

of cyber crime victims say **they didn't report the incident**.

48%

of participants said they **have never heard of MFA.**

64%

of the participants **reported not having access to cybersecurity training.**

Nearly 25%

of respondents **don’t perceive cybersecurity practices as a high priority.**

21%

We found **generational differences in the reporting behaviors of the victims** of cybercrime and identity theft.

Gen Zers were the **least likely to report** cyber crime incidents.

33%

of people **still don't routinely install software updates** as soon as these are available.

Over a third 39%

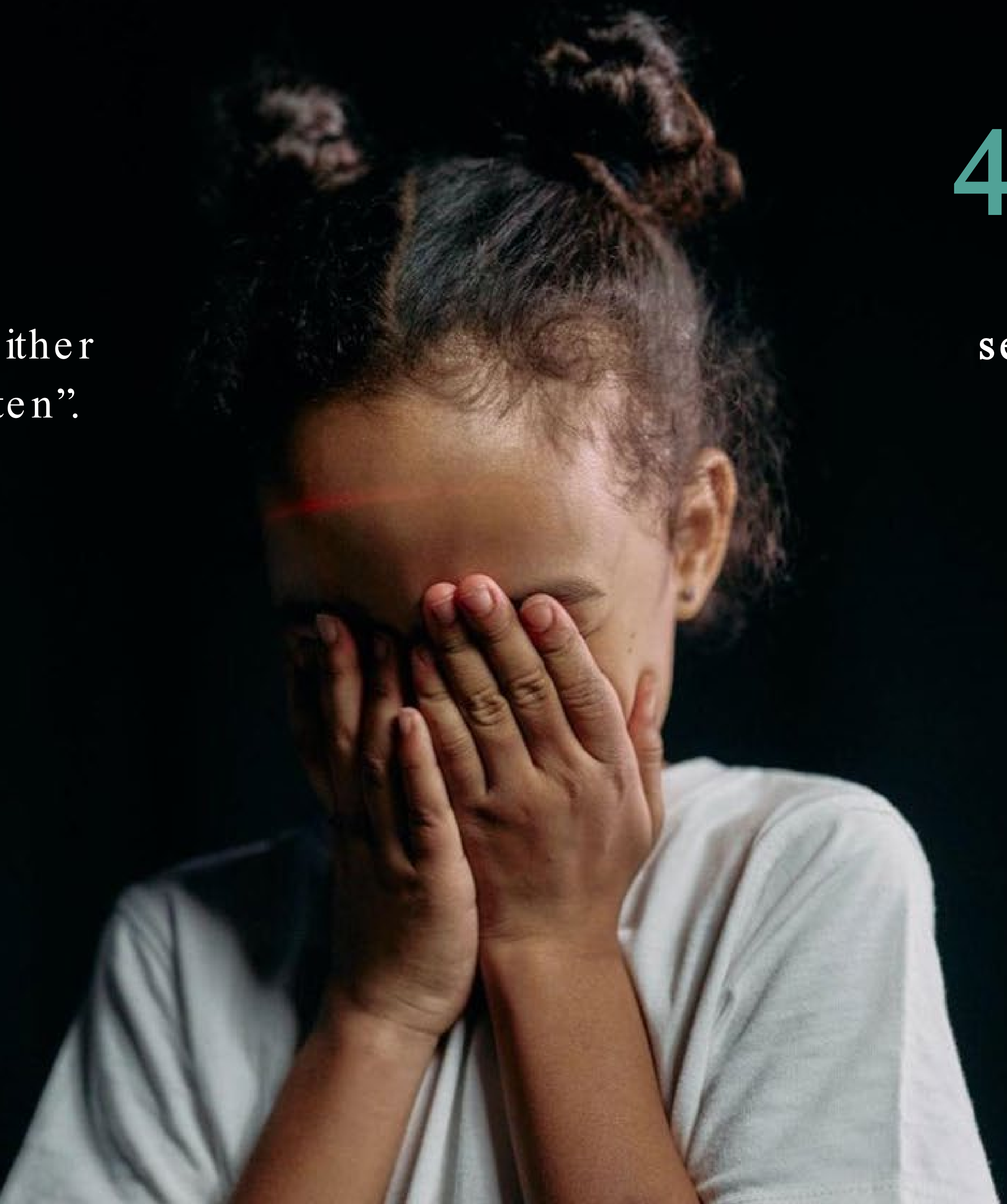
of the full-time and part-time employees participating **perceived themselves to be the least responsible** for protecting workplace information.

43%

create a **long and unique password** either "always" or "very often".

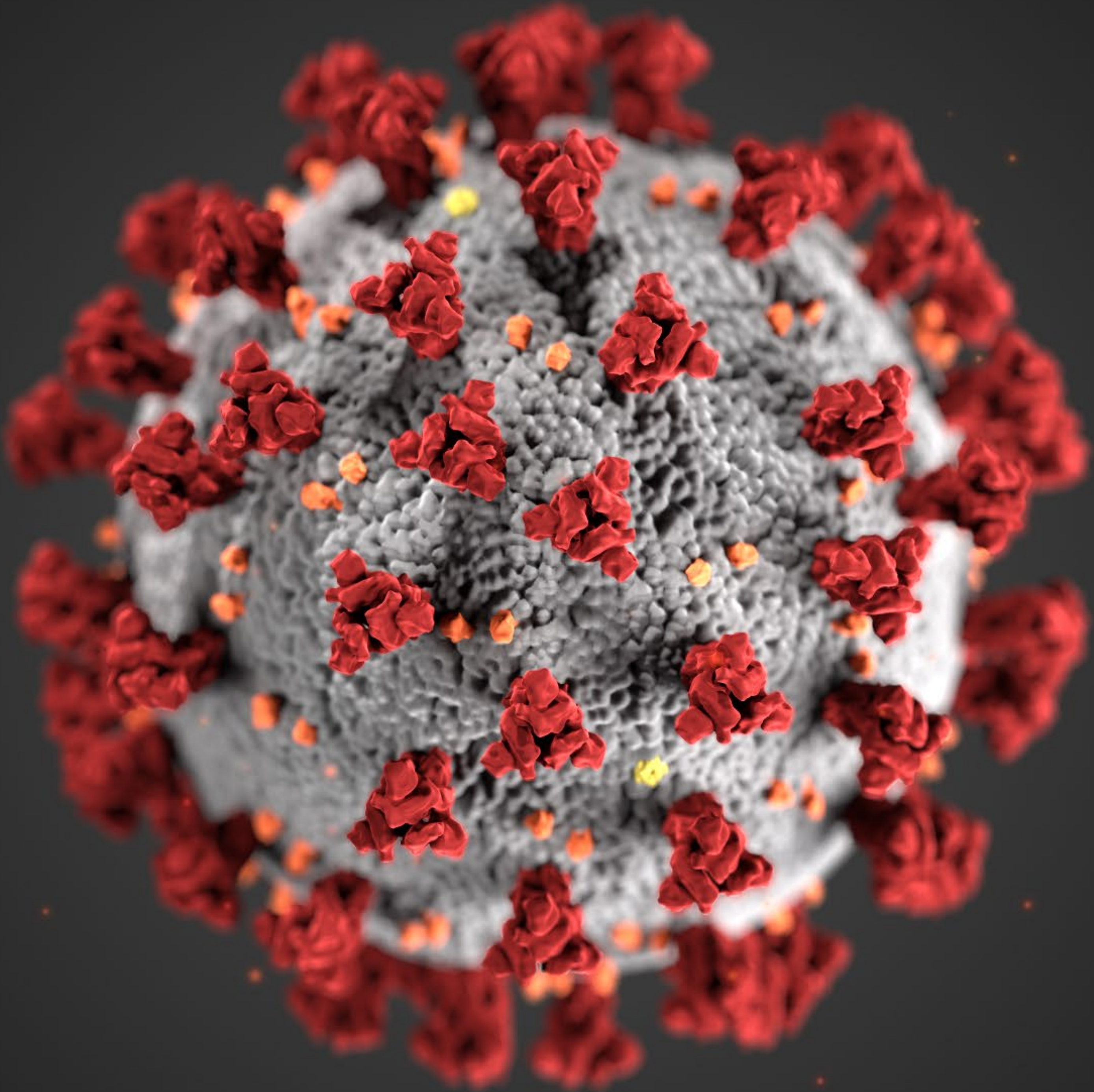
41%

stated they find **staying secure online frustrating**.



41%

reported feelings of intimidation concerning cyber security matters.



Face Shield
Face Shield
18
יציאה

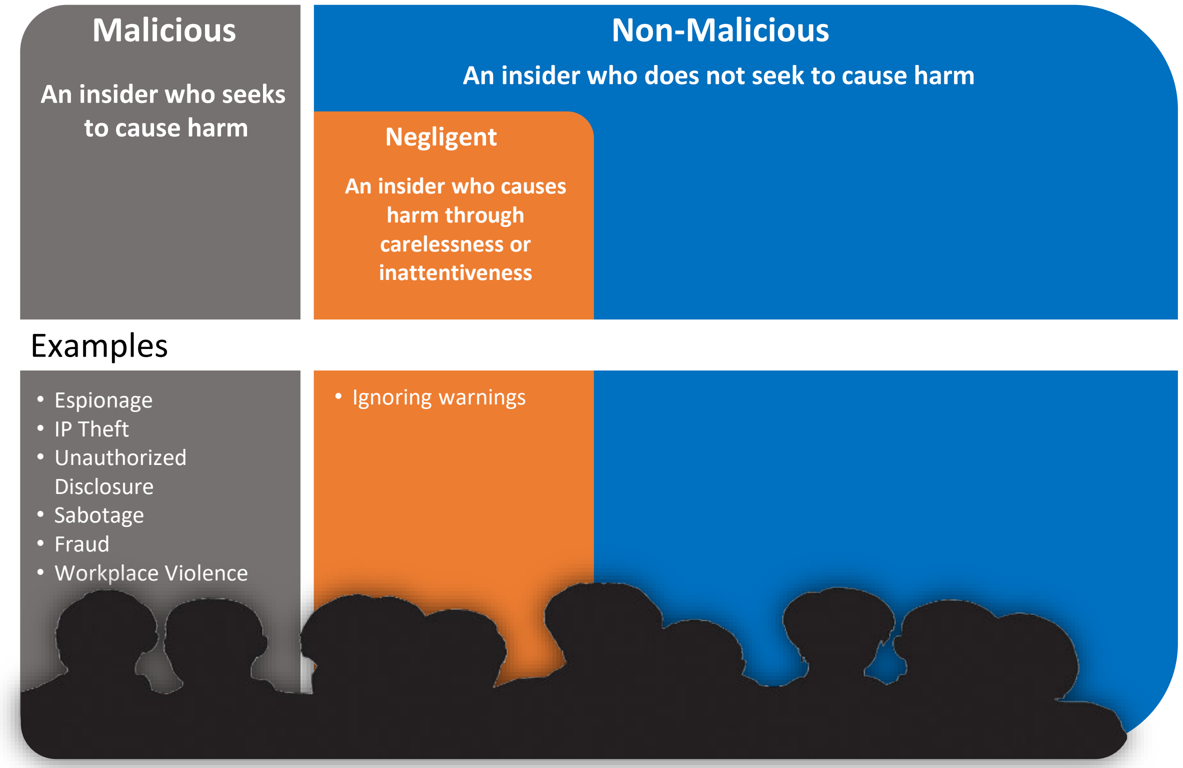
> “People are irrational and they usually make decisions that have nothing to do with facts. And yet we spend most of our time improving our facts and very little concerned with the rest.”

Seth Godin

Economic Espionage: Behavioral Study on Employee Reporting of Security Incidents

MITRE Innovation Program

Defining Insider Threats



Malicious

An insider who seeks to cause harm

Non-Malicious

An insider who does not seek to cause harm

Negligent

An insider who causes harm through carelessness or inattentiveness

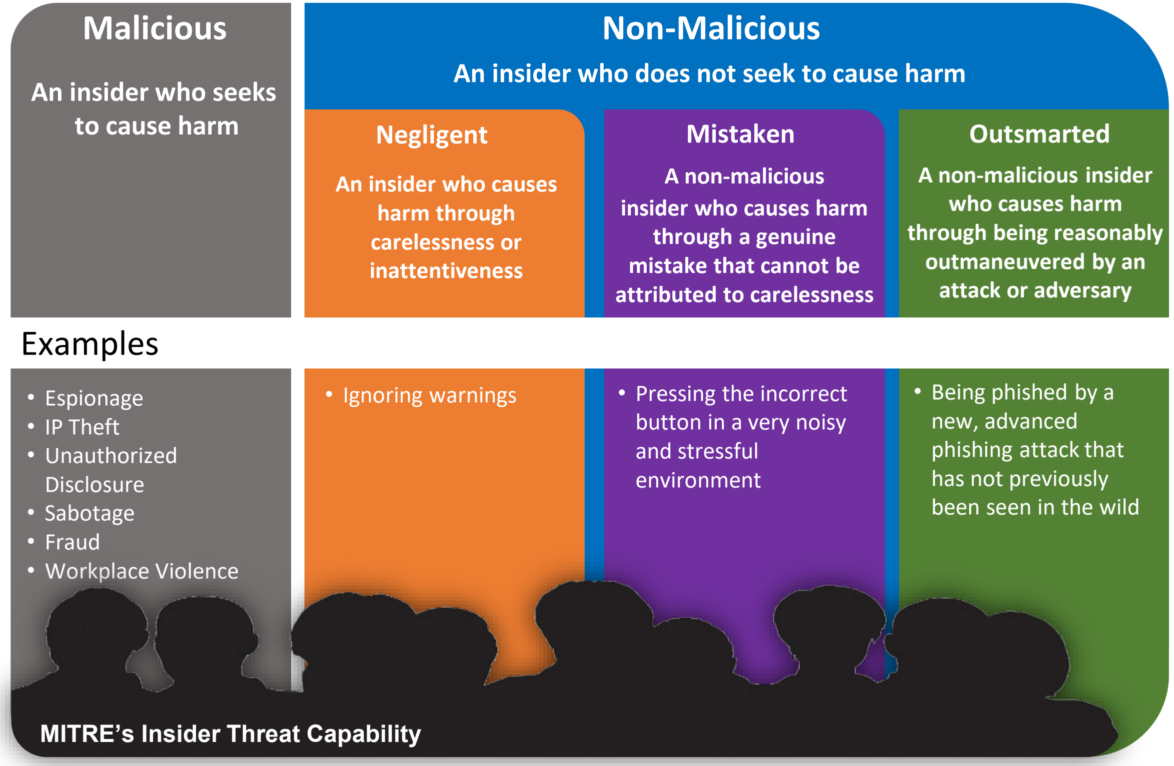
Examples

- Espionage
- IP Theft
- Unauthorized Disclosure
- Sabotage
- Fraud
- Workplace Violence

- Ignoring warnings

Security Community View of Insider Threat Types

Defining Insider Threats



Malicious

An insider who seeks to cause harm

Non-Malicious

An insider who does not seek to cause harm

Negligent

An insider who causes harm through carelessness or inattentiveness

Mistaken

A non-malicious insider who causes harm through a genuine mistake that cannot be attributed to carelessness

Outsmarted

A non-malicious insider who causes harm through being reasonably outmaneuvered by an attack or adversary

Examples

- Espionage
- IP Theft
- Unauthorized Disclosure
- Sabotage
- Fraud
- Workplace Violence

- Ignoring warnings

- Pressing the incorrect button in a very noisy and stressful environment

- Being phished by a new, advanced phishing attack that has not previously been seen in the wild

MITRE's Insider Threat Capability

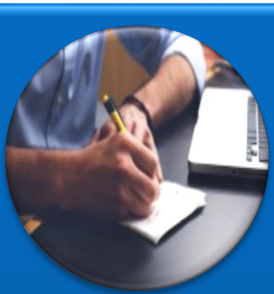
MITRE's Human-Centered Insider Threat Types

Research Problem

Insider Threat, Human Sensors, and Reporting Behavior

Insider threats can cause significant operational, reputational, and financial harm to government and industry

Human sensors (e.g., supervisors, colleagues) play a critical role in preventing, detecting, and mitigating insider threats because of their ability to report concerning behaviors and incidents that are not observable by computers or networks



Research on employee reporting of insider threats or security incidents has consistently revealed that underreporting by employees is a continuous challenge

Overarching Experimental Design Considerations

Ecological Validity

- For each environment, participants will be exposed to insider threat situations that they are likely to face in their workplace
- The research team will collect data about participants' **actual reporting behavior** (e.g., Security, Human Resources)

Experimental Condition Boundaries

- The threat situation should be obvious and **not ambiguous**
- Workplace violence or terrorism excluded

Participant Protection

- Employees **will not be penalized** for reporting or not reporting behavior resulting from the exposure environments

Design Overview and Participant Selection

Overview of Experimental Design

- Malicious actor (e.g., MITRE researcher) sequentially sends 3 pre-scripted InMail messages.
  - Messages tailored to influence participants to focus on their skillset and expertise
  - Each InMail incorporated known adversary language and behavior
  - InMails constructed to increasingly escalate recipient's concern
- MITRE follow-ups with employees for consent and one hour security interview either after receiving three messages or immediately after they report

Participant Selection Methodology

- Stratified sample of **300** employees by level (e.g., Levels 2,3,4,5,6)
- Random number generator applied to employee identification numbers to determine which employees would be exposed to the study

To ensure realism, employees were unwitting and thus unable to provide consent in advance of receiving messages

LinkedIn InMails

InMail 1
“Introduction and Interest”

- Expressed an interest in the participant’s skill and/or access to information at [Company]
- Clearly indicated a foreign nexus: China
- Mentioned generous compensation
- Asked for “confidential conversation”

InMail 2
“Quell Concern”

- Appealed to the participant (time-sensitive; legitimize failure to respond)
- Sought to alleviate any concerns or doubts about the solicitation
  - No travel
  - Part-time consulting
  - Remote
- Emphasized extra income in tough times
- Mentioned [Company’s] work on Great Powers Competition and 5G
- Re-emphasized foreign nexus

InMail 3
“Appeal and Influence”

- Appealed to the participant (missed opportunity “I would hate to miss a chance to connect”)
- Indicated already being in contact with another employee “I have been engaging with Mr. Williams, a Lead Engineer at [Company], and he has shared valuable presentations” (existing insider threat)
- Re-emphasized payment “You will be privately well compensated for your time and information sharing”
- Re-emphasized foreign nexus

Reporting Findings

Total Number of Employees Approached: 290
Total Number of Employees Interviewed: 244

Participant Types

- **61 Reporters** reported the contact
  - 58 Reporters were interviewed for the study and 3 were not interviewed
- **92 Non-Reporters** confirmed exposure to the messages, but did not report

And…

- **94 Unaware** participants received, but were not exposed to the messages
- **43 Did not report or respond** to request for interview

Reporting Rate: 35% - 39%

Employee Responses to Message

6 employees responded directly to the “fake foreign recruiter”

- “Thank you for reaching out. At this I’m only interested in full time staff positions. Also my total compensation package including salary and benefits is 200k. Please let me know if any opportunity arises for which I’d be a fit.”
- “I would be happy to meet/chat regarding the above. Kind regards”
- “Hi Brittany - thank you for reaching out. I would be happy to learn more about this role. Please let me know when would be a good time for you to chat.”
- “Hi Brittany, I can be reached at xxx-xxx-xxxx. I’m available today around 1 pm, otherwise tied up today and tomorrow. I’m available on the weekend as well.”
- “I am unclear what you are seeking. I cannot do work on behalf of [Company] that would be compensated. I am happy to talk with you if you want to set up a call. Thank you”
- “Sarah, Please remove me from your interest list.”

5 out of the 150 employees who read the first message opened the door to discussion

Paths to Reporting

Reporting Mechanism/Path for the 61 Reporters

REPORTING MECHANISM/PATH	%
Security	**91.80%**
Email: Suspicious (InfoSec)(suspicious@[Company].com)	50.00%
Named Security Personnel	21.43%
Form/Web: Report of Suspicious Activity (index/counterintelligence/report-suspicious-activity/)	17.86%
Form/Email: Suspicious Contacts and Activities (suspicious-activities-reporting-list@[Company].com)	10.71%
Leadership	**8.20%**

Recommendations

1. Reporting mechanism is not the problem
2. Both groups knew textbook response to reporting, yet their actual behaviors were not consistent with that knowledge
3. Overconfidence in ability to mitigate vulnerabilities
4. Data indicates a lack of clear understanding of "what risk" to report
5. Non-reporters do not see themselves as a target
6. Employees struggle to connect private networks with work risk
7. Reporters discussed with others more
8. Non-reporters personally know fewer people who have reported insider threats
9. Non-reporters are not sufficiently concerned about their mutual friends' networks
10. Embedding Insider Threat and CI training within general security training was not effective for recall

What We Didn’t Find

- Reporting mechanism is the problem
- Concerns with anonymity
- Fear of retaliation for reporting
- Concerns with causing trouble for other employees
- Concerns about not getting feedback from Security
    - Reporters indicated expecting follow-up after reporting
- Once a reporter, more likely to be a reporter
- Employee sensitivity to companies highly competitive strategic priorities (e.g., 5G, GPC)

Recommendations

- If your employees know how to report, focus on WHAT to report.
- Provide training and help to employees and their families and friends.
- Use security training that includes more grey-area scenarios.
- “We’re here to help” Humanize the security team.
- Be positive, skip the FUD.
- Remember COM-B and leverage emotion to motivate (storytelling, gamification, etc.)
- Remember, knowing and doing are not the same thing.