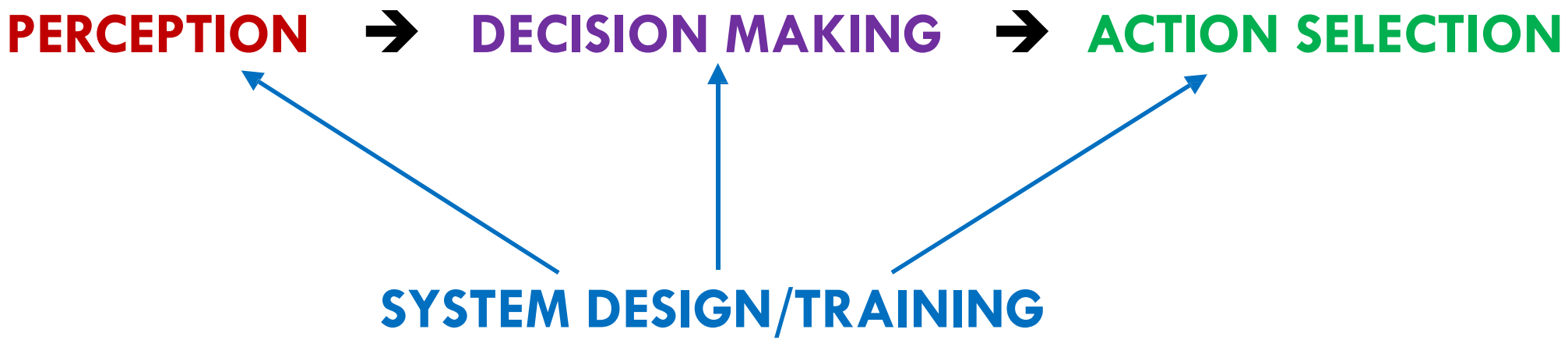
IDC6601: ORGANIZATIONS, CULTURE AND TRAINING

Institute for Simulation & Training
University of Central Florida

HUMAN FACTORS & CYBERSECURITY

1. What has Human Factors got to do with Cybersecurity?

   Scientific principles of ***perception***, ***decision making***, ***action selection***, and ***training*** that have been developed in basic and applied cognitive research can provide a principled basis for analyzing the factors affecting security-related human decisions and choices.



HUMAN FACTORS & CYBERSECURITY

PERCEPTION

- Perception of information
- Views on security, risk perception (bias, heuristics)

DECISION MAKING

- Factors that contribute to vulnerability (weapons of influence, social engineering etc.)
- Expert vs. novice decision making
- Bias and heuristics that affect decision making
- Decision making under stress, over/underload, fatigue

ACTION SELECTION

- Ease of implementing response required

SYSTEM DESIGN

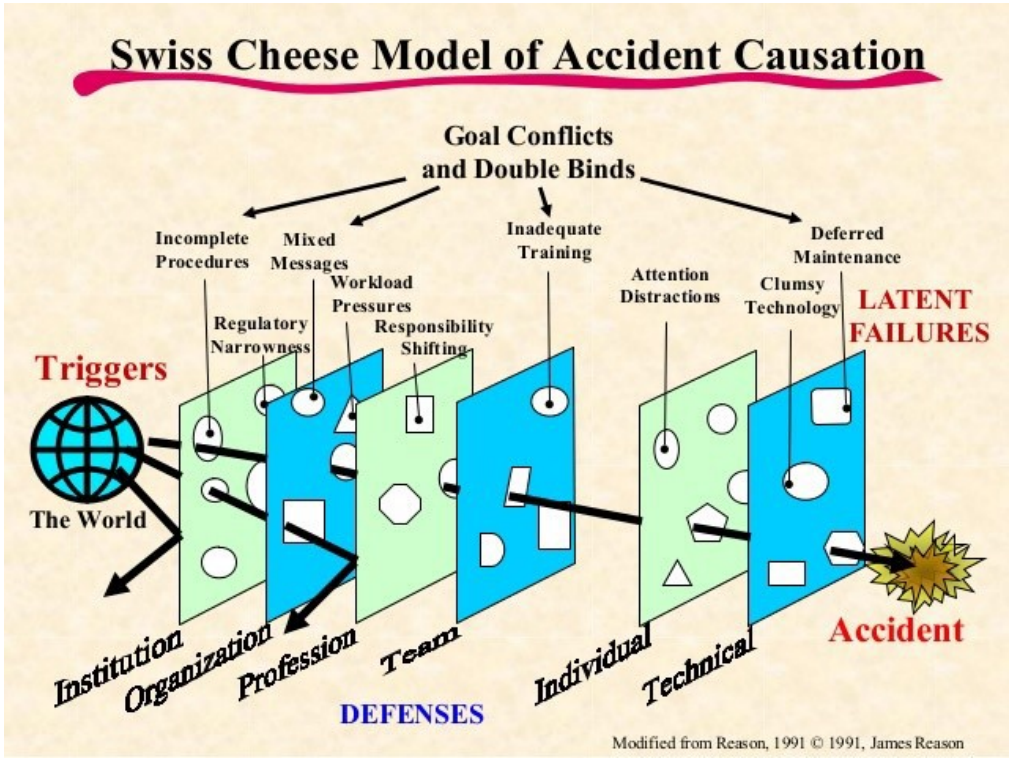
- Features of task, website etc.

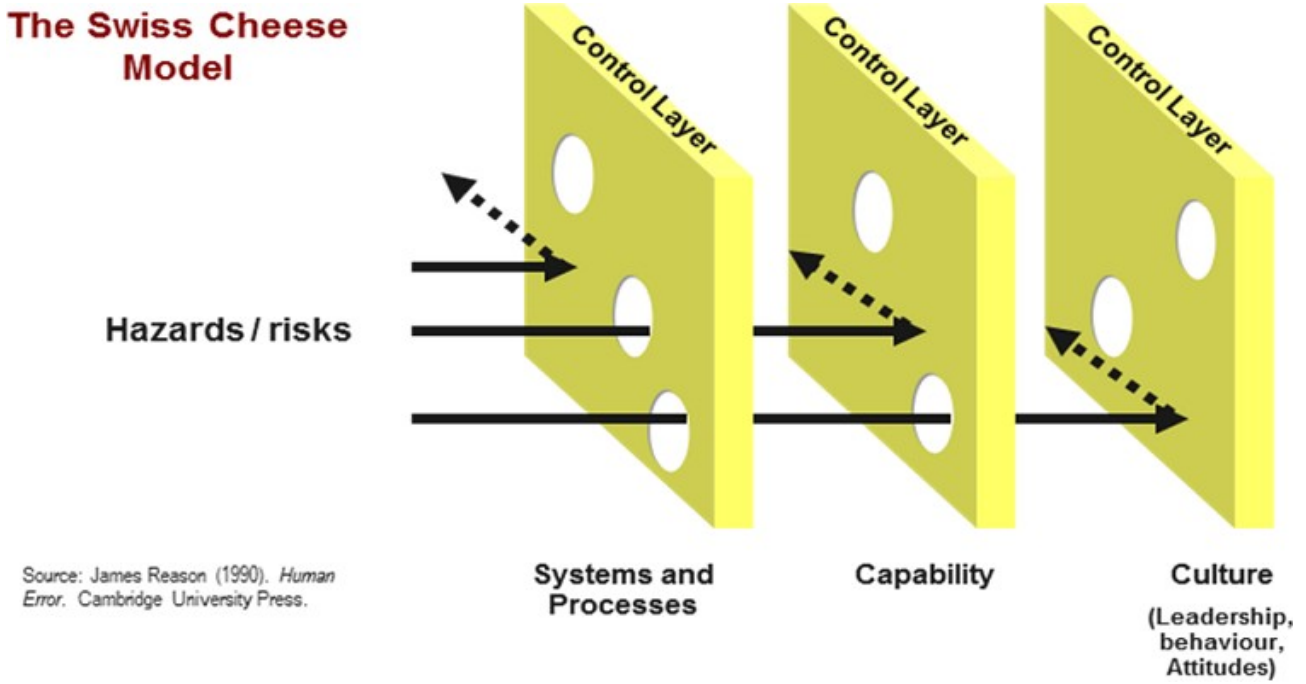
TRAINING

- Organizational factors

HUMAN FACTORS & CYBERSECURITY

- Reason's (1990) Swiss Cheese model





HUMAN FACTORS & CYBERSECURITY

- Security requires an on-going effort. It does not stop when you've purchased the latest and greatest securities technologies or even when you've conducted awareness training for staff. There are new threats everyday; three questions to consider:

Is the right **TECHNOLOGY** in place?
(i.e., applications, architecture, infrastructure)

Are the right **PEOPLE** in place?
(i.e., roles & responsibilities, culture & attitudes, skills & training, organization)

Are the right **PROCESSES** in place?
(i.e., procedures, standards, compliance)

COMMON CYBERSECURITY MISTAKES MADE BY ORGANIZATIONS

KPMG (2016) report:

1. **"We have to achieve 100% security"**
   - Impossible to achieve 100% security. Cyber threats are "here to stay".
2. **"When we invest in best-of-class technical tools, we are safe"**
   - Tools are essential, and have to be integrated into the technology architecture, but they should not be the drivers of cybersecurity strategy.
   - The best tools are useless if no one can/wants to use it properly. Importance of organizational factors.

COMMON CYBERSECURITY MISTAKES MADE BY ORGANIZATIONS

KPMG report (con't):

3. "Our weapons have to be better than those of the hackers"
   - Security policies should be determined by organization's goals, not by hackers
   - Need to understand value of assets and conduct risk assessment that drive security strategies.
4. "Cybersecurity compliance is all about effective monitoring"
   - The ability to learn is as important as the ability to monitor
   - Organizations have to continually learn about external developments and new threats, learn from incidents, learn about what affects risk. Then organization will be better informed to make appropriate security policies.

COMMON CYBERSECURITY MISTAKES MADE BY ORGANIZATIONS

KPMG report (con't):

5. "We need to recruit the best professionals to defend ourselves from cybercrime"
   - Cybersecurity is not a department, but an *attitude*. It should be mainstream throughout the company – i.e., part of HR policy, development of IT systems, project management etc.

ORGANIZATIONAL CULTURE

- **What is organizational culture?**
  - "Attitudes, values, beliefs, norms and customs of an organization"
  - "Outcome of conversations and negotiations between members"
- **Organizational culture can be:**
  - Focused on negative motivators – fear of penalty, paranoia
  - Focused on positive motivators – openness, trust, empowerment

  ➔ *In general, reward is more powerful than punishment*

ORGANIZATIONAL CULTURE

- Often, changes to improve security culture comes ***after*** an incident
  - Management trying to cope with damage/embarrassment
  - React to "show that something is getting done" quickly
  - Blame-shifting, excessive caution (e.g., new annual training for phishing)

These can lead to…

➔ *Tone of negativity, culture of fear and paranoia, development of "Blame Culture"*

➔ *Discourage risk taking and honest reporting of factors that might contribute to further incidents*

➔ *People may be more cautious, but it will not eliminate the honest mistakes caused by poor process design*

➔ *Remedial action may not focus on the true, underlying factors (i.e., lack of supervision, training, stress, unrealistic time pressure/deadlines that encourage expedient behaviors, poor system design)*

CHANGING BEHAVIOR

- Common techniques and interventions used to bring about organizational changes:
  - Management by objectives
  - Survey feedback
  - Team building
  - Six Sigma
  - Quality circles
  - Total Quality Management
  - Etc…
- As much as organizations can over-rely on security **tools** to defend against cyber-attacks, they can over-rely on these interventions and **processes** to change behavior.
- Many of these target processes and change at the *organizational level* and do not easily translate to changing behaviors at the *individual level* (Whelan-Berry, Gordon, & Hinnings, 2003).

CHANGING BEHAVIOR

- Fostering **behavioral change** in individuals involves **changing attitudes** and **providing knowledge**
  - Knowledge
    - Easiest to convey
    - Can be externally imposed
  - Attitudes
    - More difficult to change
    - Although rules, policies and instructions can affect certain attitudes, these are still inadequate
    - Attitudinal change usually requires internal processing by the individual
  - Behavior
    - Hardest of all to modify, as there are multiple factors, including situation at the moment
    - Consequences can be effective in changing behaviors

CHANGING BEHAVIOR

- Understanding why people do what they do (or don't)
  - E.g.,
  - Why do/don't people seek preventative health care? (e.g., health screenings)
  - Why do/don't people make healthier food choices?
  - Why do/don't people exercise regularly?
  - Why do/don't people engage in safe sex?
  - Why do/don't people buckle up in cars?
  - Why do/don't people drink and drive?
  - Why do/don't people perform regular backups?
  - Why do/don't people share their passwords?
  - Etc…

THEORIES OF BEHAVIORAL CHANGE

- **Social Cognitive Theory (Bandura, 1986)**
  - Personal factors, e.g.,
    - **Emotional Coping** — The ability of an individual to cope with emotional stimuli
    - **Self-efficacy** — A judgment of one's ability to perform the behavior.
    - **Self-Control** — The ability of an individual to control their behaviors

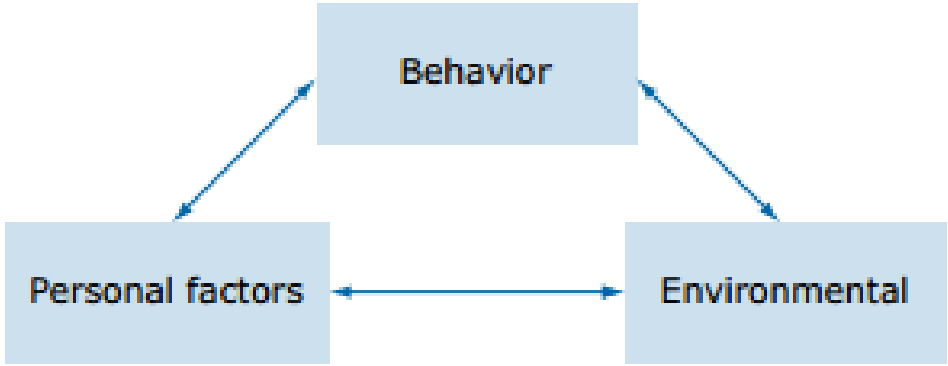


Figure 1. Social Cognitive Theory Model

  - Environmental factors, e.g.,
    - **Reinforcements** — Something that increases or decreases the likelihood a behavior will continue
    - **Observational Learning** — Behavior acquired from observing actions and outcomes of others' behavior
    - **Outcome Expectations** — A judgment of the likely consequences a behavior will produce. The importance of these expectations (i.e., expectancies) may also drive behavior.

THEORIES OF BEHAVIORAL CHANGE

- **Theory of self-efficacy (Bandura, 1977)**
  - Behavior depends on:
    i. The realization that there is risk
    ii. The expectation that the behavior will reduce risk
    iii. The belief in one's ability to engage in the right behavior or avoid the wrong behavior
  - Individuals with high self-efficacy think that they can shape outcomes
  - Individuals with low self-efficacy don't think that they can affect what happens

- **Expected utility hypothesis (Bernoulli, 1954)**
  - Behavioral change depends on the extent to which the individual perceives the behavior as being useful/bringing utility.

CHANGING BEHAVIOR

- Changing behaviors at the individual level ≠ changing behaviors of individuals ***within an organization***
  - Impact of being in a group, part of an org. structure
  - Impact of authority/hierarchy
  - Impact of one's work on others/entire product
  - Impact of work environment
  - Impact of work schedules and deadlines
  - Impact of organizational rewards and sanctions
  - Etc.

CHANGING BEHAVIOR IN ORGANIZATIONS

Awareness campaigns

- Awareness is to make people amenable to change.
- Why majority of security awareness campaigns do not work (Bada & Sasse, 2014)
  - Awareness is not training, it merely focuses attention on safety
  - Solutions not aligned to business risks
  - Progress and value of change not measured
  - Unrealistic expectations
  - Correct skills are not deployed

CHANGING BEHAVIOR IN ORGANIZATIONS

Beyond awareness campaigns

- Relevant processes in *influence*: Central vs. Peripheral route, dual processes, weapons of influence etc.
- Communication (in the organization) occurs all the time
  - Communications does not happen only someone says/does something. *NOT* saying/doing is also communicating.
  - Message from official communications can be superseded that from unofficial communications (e.g., seeing others engage in unsafe cyber behavior without negative consequences)

CHANGING BEHAVIOR

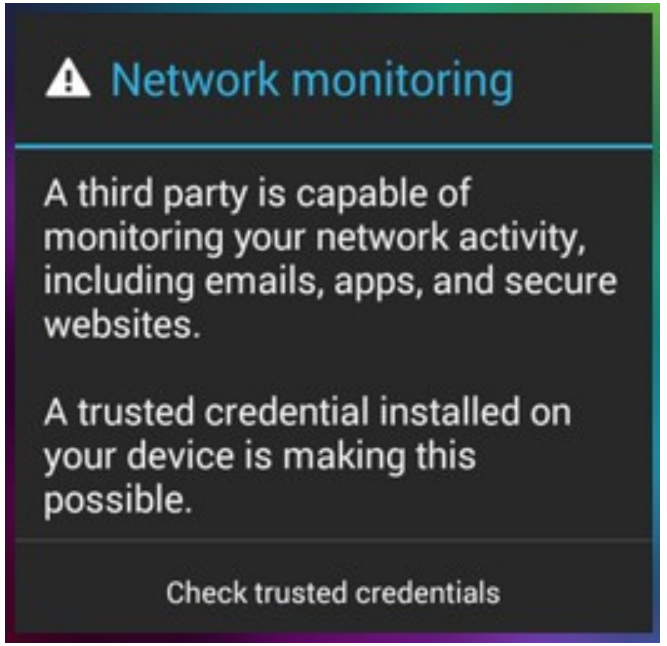
- 10 factors that most influence organizational attitudes and behavior (Lacey, 2009):
  1. Personal, real-life experiences
     - Individual's or others'
  2. What the individual thinks is their role in the organization
     - "I'm just a lowly helpdesk assistant" vs. "I help defend against cyber crime"
  3. Cues in the local office and cyberspace environment
     - E.g., unlocked PCs at workstations, visitors to company given free access, lax policies about taking company laptops home etc.

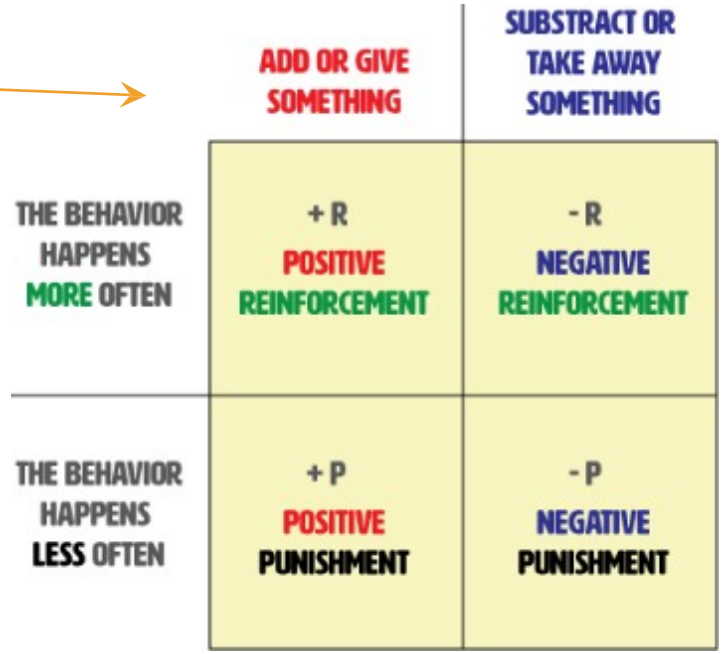
CHANGING BEHAVIOR

- Factors that most influence organizational attitudes and behavior (con't):
  4. Actions of immediate coworkers
     - Vicarious learning, social modeling
  5. Influence and authority of the management
     - Leadership sets the tone
  6. Accepted corporate rules and procedures
     - Importance of appropriate security policies and procedures

CHANGING BEHAVIOR

- Factors that most influence organizational attitudes and behavior (con't):
  7. Cues and controls in the systems used
  8. Most recent experiences
  9. Consequences of actions
  10. Events, things that are personal, immediate and certain





CHANGING BEHAVIOR IN ORGANIZATIONS

These lists of factors can generally be classified into:

- **Social factors**
- **Environmental factors**
- **Individual factors**

CHANGING BEHAVIOR IN ORGANIZATIONS

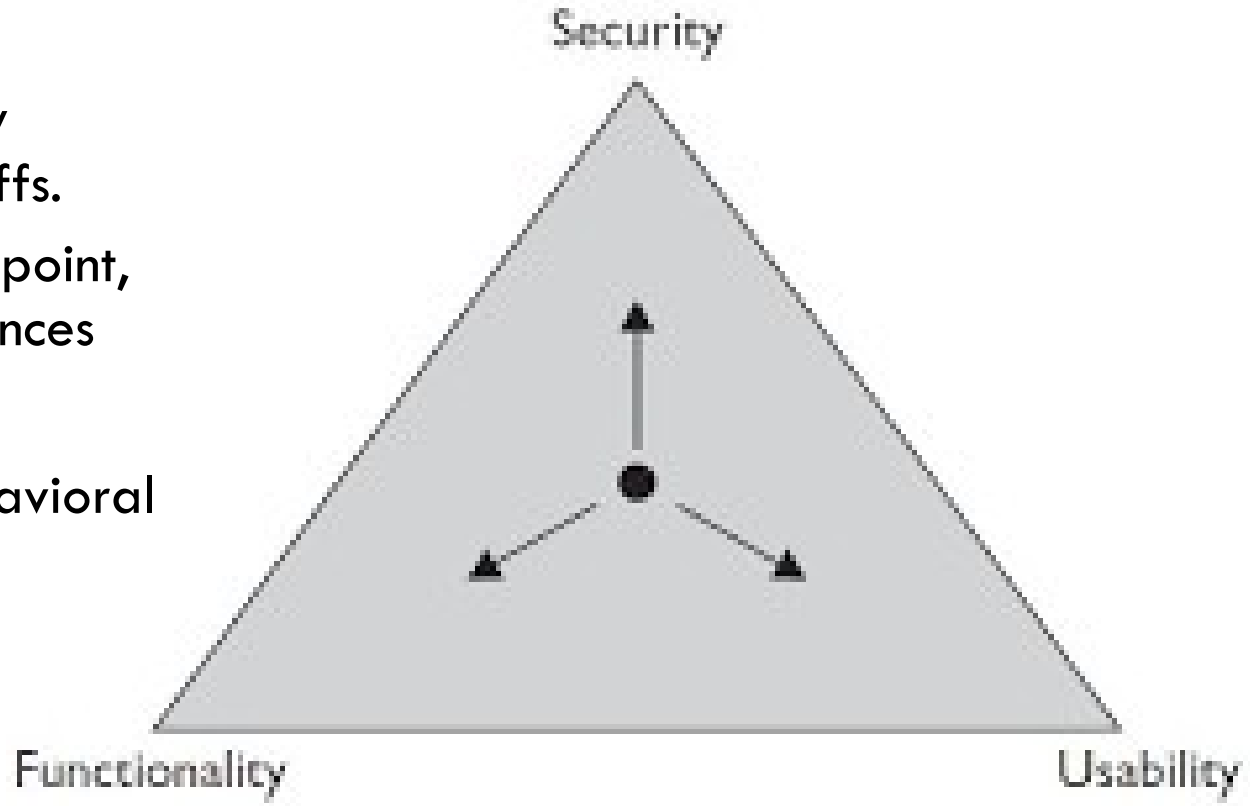
- **Social factors**
  - Peer pressure and social norms within the organization/team
  - Leadership plays a key role in fostering a security culture (Coventry et a., 2014)
- **Environmental factors**
  - Default settings and pre-sets in system
  - Physical accessibility to computers and servers etc..

CHANGING BEHAVIOR IN ORGANIZATIONS

- **Individual's motivational orientation, cognitive and affective characteristics**
  - Messages are more persuasive when they:
    - Match the individual's regulatory focus, which makes message "*feel right*" (Uskul et al., 2009; Cesario et al., 2004)
      - Regulatory focus theory (Higgins, 1998): individuals' behaviors are guided by a desire to align one's actual and "ideal" self, and involves fulfilling duties and obligations (i.e., strive to be consistent)

CHANGING BEHAVIOR IN ORGANIZATIONS

- **Individual's characteristics (con't)**
  - Security fatigue
    - Designers of systems and security policies must consider the tradeoffs.
    - Each person has own equilibrium point, which may change with circumstances
  - Fear
    - Can lead to attitude and/or behavioral change (Girandola, 2000)



ORGANIZATIONAL SAFETY/SECURITY CULTURE

- Parallels drawn between safety culture in the cyber domain and safety culture in industries like healthcare, construction, mining, aviation, manufacturing etc. (i.e., physical safety)

  Physical safety culture

  - Zero incident: the only acceptable target is 0 accidents
  - Near-miss reporting and feedback
  - ABC behavioral analysis

    : Antecedent → Behavior → Consequence

ORGANIZATIONAL SAFETY/SECURITY CULTURE

- A safety/security culture is a culture where there's
  - Transparent communication
  - Acknowledgment of risks
  - Understanding of the link between individual behaviors and larger outcomes
  - Commitment of resources to address safety concerns
  - Encouragement of collaboration across ranks to seek solutions
  - Problem-solving mindset instead of blame-shifting
    - an environment where individuals are able to report errors or near misses without fear of reprimand or punishment.
    - place emphasis on the unsafe behavior that violates policy, not the outcome (so should penalize unsafe behavior even when outcome is benign)

ORGANIZATIONAL SAFETY/SECURITY CULTURE

- Factors involved in fostering a physical safety culture are similar to that for a cyber safety culture:
  - Management commitment
  - Work pressure
  - Reporting system
  - Etc…
- However, there is ONE major difference (esp. for high-value networks/servers etc.)…there is an ***adversary*** in the cyber domain

CHANGING BEHAVIOR

- So how does learning about behavioral changes in individuals, training, organizational culture help?…it takes only **ONE** wrong behavior/action to trigger a devastating cyberattack

ORGANIZATIONAL TRAINING

- **What are the knowledge, skills and abilities to train for in the cyber domain?**
  1. For Analysts & Defenders: e.g., attribution training, training on defensive, restorative action etc.
  2. For all Users: e.g., train on knowledge and methods of attacks

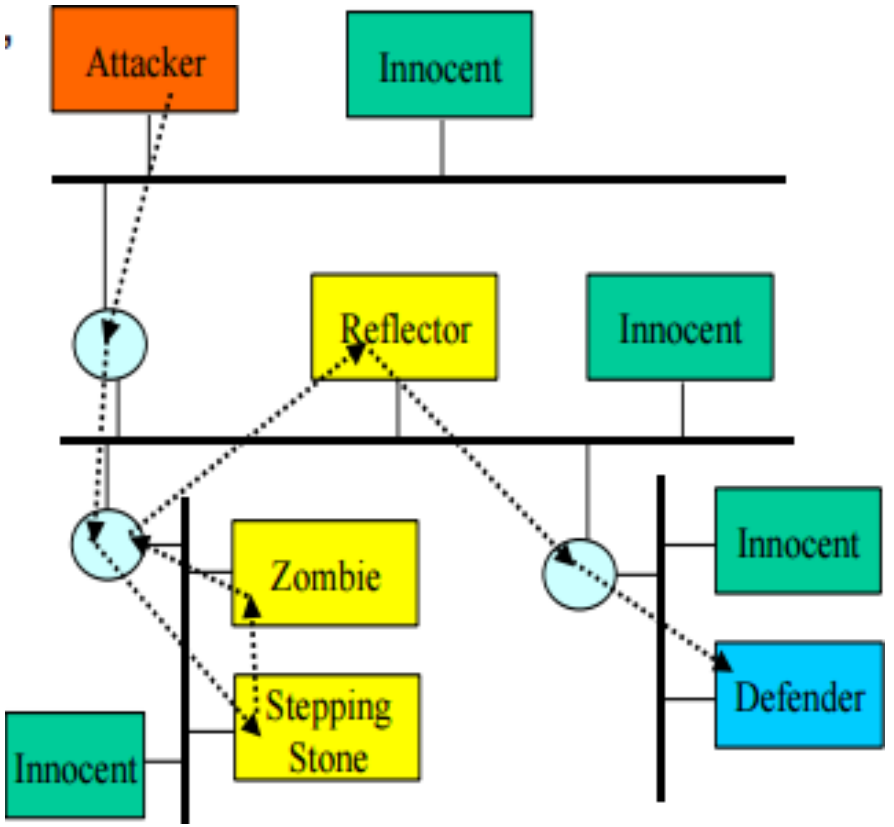
TRAINING: ANALYSTS & DEFENDERS

E.g., Attribution training

- Attribution: being able to detect and deduce where the attack is coming from
- Consequences of misattributions: misdirected actions taken that (i)can harm "innocent" systems that were used to rout the attack, (ii) fail to stop attack (Graham, 2010)
- Difficult to attribute/trace attacks because identities can be easily masked in cyberspace.

TRAINING: ANALYSTS & DEFENDERS

- Attribution is especially difficult because of attackers have the ability to do the following in cyberspace (Wheeler, 2013):
  1. Spoof
  2. Use Reflection,
  3. Use Laundering hosts (e.g., stepping stones, zombies, botnets)
  4. Take advantage of timeframes (ms to months)



TRAINING: ANALYSTS & DEFENDERS

- Attribution is also difficult if defense relies heavily on passive defense tools (e.g., firewalls, encryption, anti-virus) that merely block the attack but do not collect data that may reveal attack origin and identity of attacker.
  - Anonymity →Low deterrence (attackers can simply try and try again)
  - Anonymity in cyberspace linked to political ideologies (e.g., right to free speech)
    - Is there/Should there be an acceptable level of surveillance that can be implemented across the board?

TRAINING: ANALYSTS & DEFENDERS

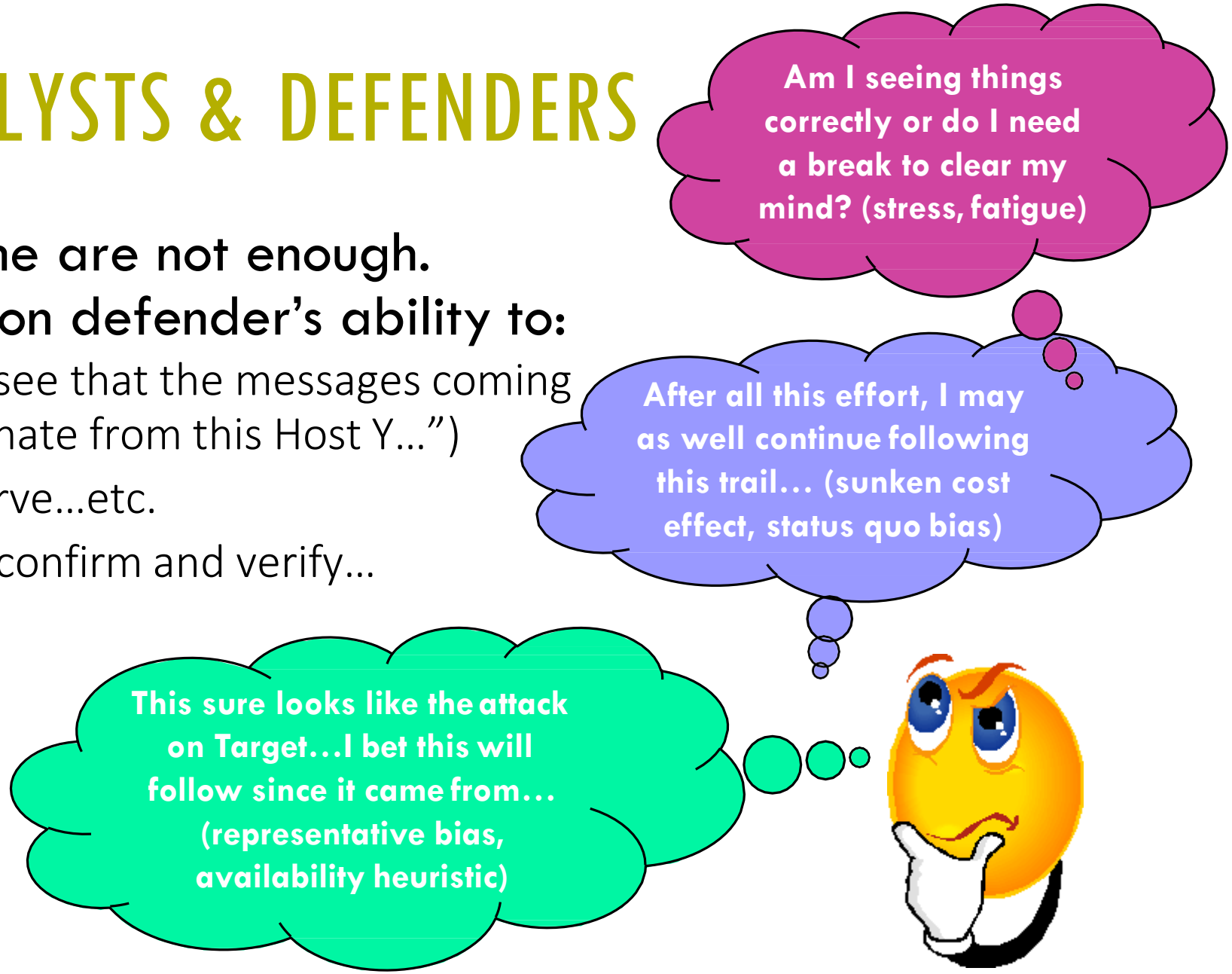
- Attribution techniques include using logs, trackback queries, debugging input, querying/monitoring hosts, filtering, tag messages going through routers etc.
- Techniques can also be classified according to the following (Vandenberg, 2014):
  - Route-based methods (e.g., ingress filtering, traceback)
  - Packet-based methods (e.g., packet logging, modify transmitted message)
  - Target-based methods (e.g., hackback, honeypots)
- Should use different techniques effective for different attack types

TRAINING: ANALYSTS & DEFENDERS

- **Techniques/methods alone are not enough. Attribution still depends on defender's ability to:**
  1. Observe and detect that something is happening/has happened (e.g., "people are getting emails with strange attachments")
  2. Formulate some hypotheses (e.g., "Router X may be used to transmit attachment containing macro that has malicious script)"
  3. Determine the data to collect and act to obtain data (e.g., "Mark messages that come through Router X…")

TRAINING: ANALYSTS & DEFENDERS

- Techniques/methods alone are not enough. Attribution still depends on defender's ability to:
  4. Analyze the data (e.g., "I see that the messages coming to Router X seem to originate from this Host Y…")
  5. Collect more data….observe…etc.
  6. Deduce origin of attack…confirm and verify…



TRAINING: ANALYSTS & DEFENDERS

- All this sounds like…

TRAINING: ANALYSTS & DEFENDERS

- …and supports the case for ***COMPETENCY-BASED TRAINING****, not attack type-based training.*
  - Competencies are the measurable or observable knowledge, skills, abilities, and behaviors (KSABs) possessed by the individual that are critical to successful job performance.
  - Develop a competency model for a particular job (e.g., job of cyberdefender/investigator/analyst)
    - Conduct job, task analyses (e.g., job involves attribution)
    - Identify competencies required to perform those tasks in the job (e.g., attribution is an investigative activity which requires strong detail-orientation, ability to think critically and logically, extensive knowledge of cyber system infrastructures etc…)
      - Most competency models of cyberdefenders focus on technical knowledge rather than on logical thinking, reasoning skills

TRAINING: ANALYSTS & DEFENDERS

- Some competencies to train (or select) for in a cyberdefender:

Competency	Description
Knowledge of info. Systems/network security	Knowledge of network security architecture concepts, including topology, protocols, components, and principles
Knowledge of human factors	Knowledge of Human-Computer interaction principles
Critical thinking ability	Conducting vulnerability scans and recognizing vulnerabilities in security systems
Ability to develop software and program	Design and build system tools for detection, validation
Modeling and simulation skill	Skill in creating and utilizing mathematical or statistical models
Etc….	Etc…

TRAINING: ALL USERS

- **For all other users (with different job scopes), cyber training may include:**
  - Knowledge: E.g., Social engineering tactics, anti-spear phishing training, password and data protection
  - Skills…
  - Abilities…

TRAINING: ALL USERS

E.g., Knowledge training

- **Anti-Spear-Phishing training**
  - Train on how phishing gives access to attacker.
  - Train on knowledge of company policy on emails, links, and attachments
  - Automated computer programs that send emails to employees from Web site addresses to see who will unwittingly click on the links (e.g., the anti-spear phishing training offered by a company called Phishme, available at http://phishme.com/ the-phishme-advantage/roi/)
  - Keep records of successes and failures. Incentivize with rewards.

TRAINING: ALL USERS

E.g., Knowledge training (con't)

- **Password Protection & Awareness**
  - Train on importance of changing password regularly,
  - Knowledge of the characterisics of keyloggers and dictionaries – impact kind of password chosen
  - Mandatory changing of passwords
- **Data Protection**
  - Train on least-access principles and privilege control
  - Knowledge of software patches and critical updates (should not delay installation for lack of time/budget)
  - Responsibility of certain data lies with employee

TRAINING: ALL USERS

- Given the pervasiveness of IT and computers in today's workplace, what are some of the (other) knowledge, skills, and abilities related to the cyber domain that all employees who use computers in their jobs should have?

TRAINING PRINCIPLES

Training principles for acquiring **knowledge** (declarative knowledge)

1. **Strategic use of knowledge: leverage existing knowledge**
   - Associate new knowledge with prior knowledge incorporates the new knowledge into existing mental models/representations (Johnson-Laird, 1983)
2. **Training difficulty: certain types of "difficulties" encountered in learning may help retention and transfer**
   - Difficulty should be from a secondary task that is *relevant* to the main task and the tasks occurred *sequentially* (i.e., does not compete with primary task for resources)
     - Helps engage task-relevant cognitive processes (McDaniel & Einstein, 2005)

TRAINING PRINCIPLES

Training principles for acquiring **skill** (procedural knowledge)

1. Mental practice
   - Mental practice can retard forgetting and promote transfer of training. Physical practice may suffer from motoric interference
2. Cognitive antidote
   - Adding some cognitive complexity can mitigate adverse effects of routine tasks done over a prolonged period.
   - Complicating a boring procedure can dissipate the boredom and prevent "underload", improving performance

ORGANIZATIONAL TRAINING

But why do some very good training programs still fail to result in organizational change?

- Training has to be integrated into, and supported by, the organization's culture
- Training and organizational preparedness must go hand-in-hand with risk management and threat assessment/analysis
  - Threat analysis – can't eliminate risk entirely (not all threats can or should be countered). Instead have "acceptable risk" level
    - Manage risk in relation to:
      - Threats that exist
      - Attractiveness of target (motivation, intent, goal)
      - System vulnerabilities and access points
      - Impact of attacks
      - Safeguards to minimize impact
      - Tools and capabilities of attacker (how realistic is this?)

ORGANIZATIONAL TRAINING

- How can organizations prepare themselves to better deal with cyber threats which are very possibly the "new normal" in the near future?
  - May require a paradigm shift in how we live and work
- Can we fully make sense of/understand what happens in the cyber domain?
  - Draw from disciplines such as information systems, cognitive science, organizational psychology

IDC6601: ORGANIZATIONS, CULTURE AND TRAINING

Institute for Simulation & Training
University of Central Florida