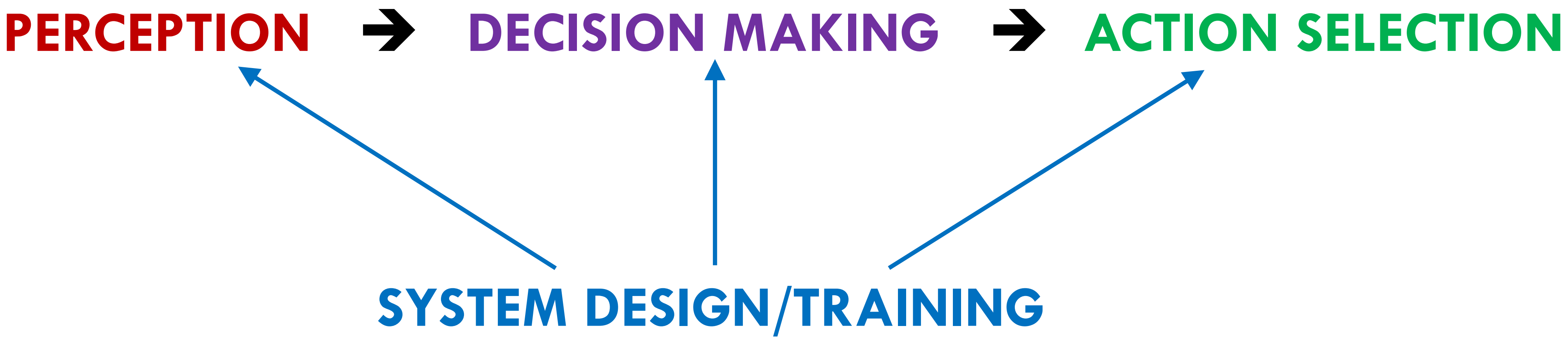
IDC6601: Processes and Motives Involved in Cyberattacks

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” (Proctor & Chen, 2015, pp. 722)



PERCEPTION → **DECISION MAKING** → **ACTION SELECTION**

SYSTEM DESIGN/TRAINING

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

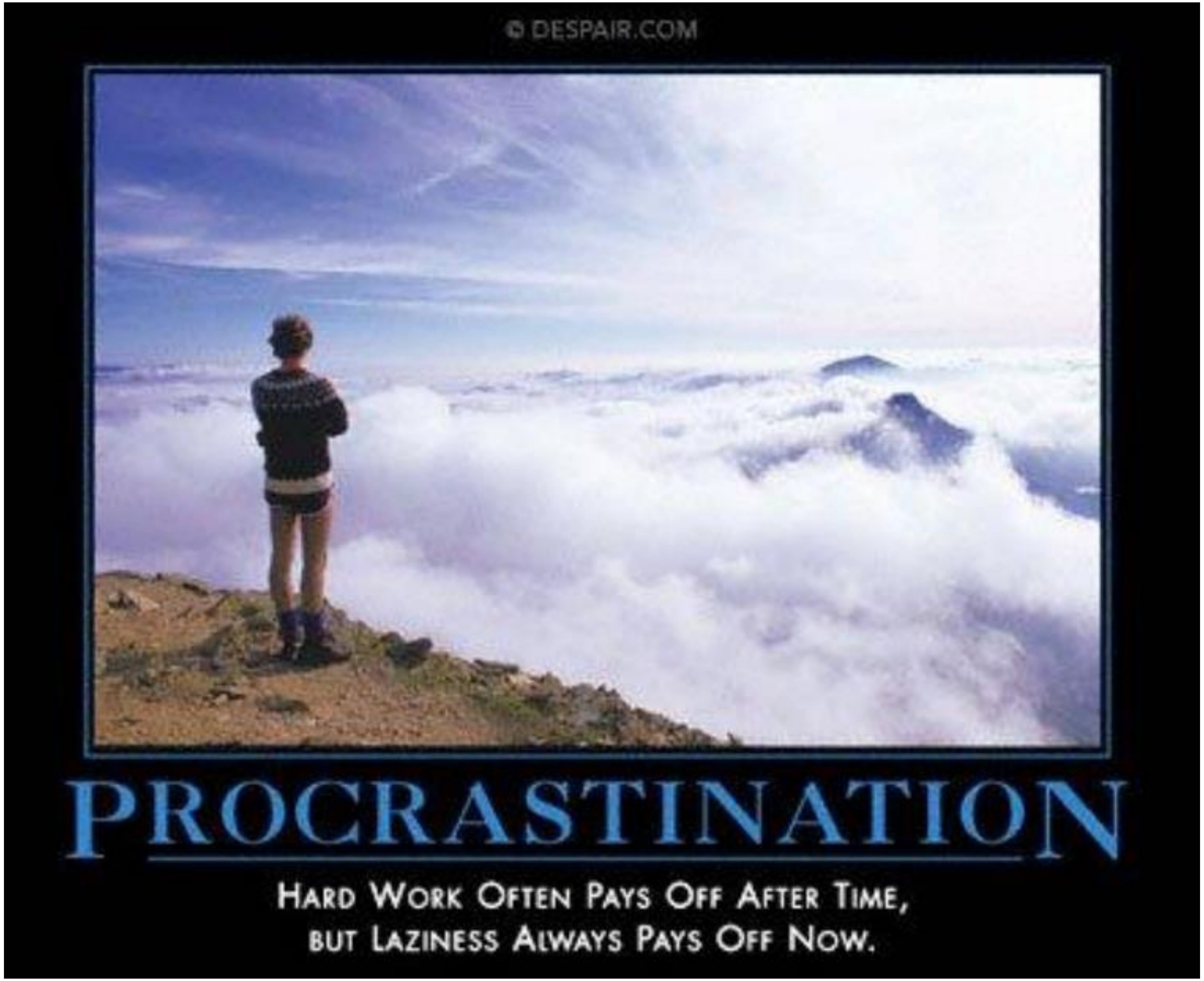
- Organizational factors

DM BIASES & HEURISTICS

- The main biases and heuristics in DM are:
  - Framing effects (i.e. Prospect Theory – Tversky & Kahneman, 1979)
  - Optimism bias (Weinstein, 1986): “it won’t happen to me.”
  - Control bias/Illusion of control (Langer, 1975): “an expectancy of a personal success probability inappropriately higher than the objective probability would warrant.”
  - Confirmation bias (Plous, 1993; Lewicke, 1998)

DM BIASES & HEURISTICS

- Status quo bias (Samuelson & Zackhauser, 1988)
  - Careful about what is set as the “default”
- Present bias, time discounting and procrastination (O’Donoghue & Rabin, 1999): intentions and plans made about future action tend to change as the future becomes the present. This is because of the tendency to over-value immediate rewards at the expense of long-term intentions
  - e.g., “I’ll back up my files/perform updates/do virus scan later”…then when later comes around, we place more value on the time freed up from not taking that action…and procrastinate.


© DESPAIR.COM
PROCRASTINATION
Hard Work Often Pays Off After Time,
but Laziness Always Pays Off Now.

FACTORS AFFECTING DM

- **Person factor** (i.e., personality traits of the Big Five)
- **Other factors**
  1. Level of Stress
  2. Whether person is in a Group setting
  3. Organizational environment, culture, policies
  4. Etc…

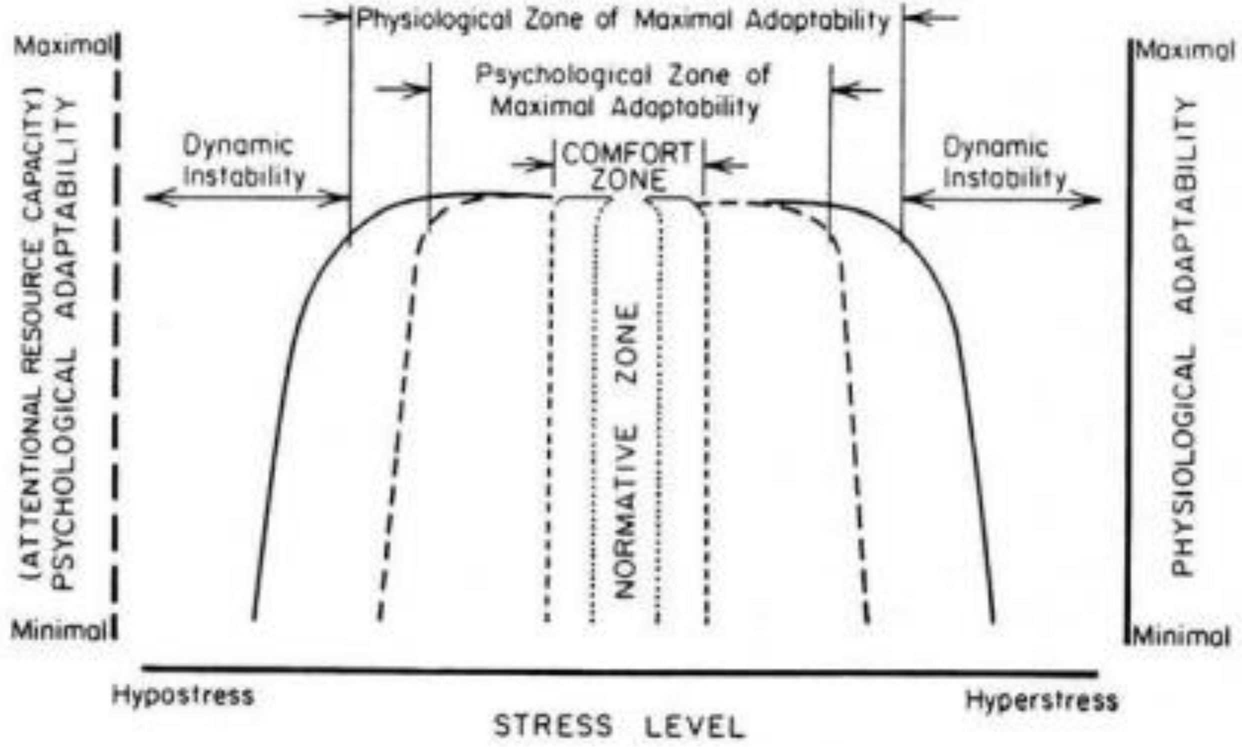
DM: PERSON FACTOR – PERSONALITY

- Personality traits (some hypotheses with vulnerability in social engineering – Uebelacker & Quiel, 2014)
  - Extraversion: higher sociability and excitement-seeking, may be tend to violate security policies, take risks
  - Conscientiousness : higher tendency to follow through with commitments, may be susceptible to continuance commitment tactics
  - Agreeableness : tend to be more trusting, may have increased susceptibility to phishing, share passwords
  - Neuroticism : greater anxiety, more cautious, may be protective, but…
    - Women who were high on neuroticism tend to fall for prize phishing email (Halevi et al., 2013)
  - Openness : tend to seek new experiences, lower concern with privacy settings
    - Those high on openness tend to post more info on Facebook, less strict privacy settings → increased phishing vulnerability (but may not relate to being actually phished) (Halevi et al., 2013)

Known as the "Big Five" personality traits

DM: OTHER FACTORS – STRESS

- Stress: ***Transaction*** between person and environment
- Performance does not decrease proportionally with increases in task demands.
  - Compensatory mechanisms
- Maximal Adaptability Model (Hancock & Warm 1989)
  - "Zones" of adaptability: psychological, physiological adaptability



Physiological Zone of Maximal Adaptability
Psychological Zone of Maximal Adaptability
Dynamic Instability
COMFORT ZONE
Dynamic Instability
NORMATIVE ZONE
Maximal
Minimal
(ATTENTIONAL RESOURCE CAPACITY) PSYCHOLOGICAL ADAPTABILITY
Maximal
Minimal
PHYSIOLOGICAL ADAPTABILITY
Hypostress
Hyperstress
STRESS LEVEL

DM: OTHER FACTORS – STRESS

- **Decision making under conditions of stress (e.g., when facing a cyberattack)**
  - In general, under stress, attention seems to *narrow*. Focus is concentrated on main tasks and reduced on peripheral information and tasks. (Staal, 2004).
  - Main task tends to be the stimuli that is most salient (e.g., threat-related)
  - People tend to focus on stimuli that most threat-relevant but may not be the most appropriate (e.g., decoy)
    - Reduces environmental scan and cue utilization, shrinks perceptive field (Wickens, 1984, Driskell, Salas, & Johnston, 1999)
    - Time distortion under stress (Hancock, Szalma, & Weaver, 2002)
    - Decision making of military personnel under time pressure: Reduced frequency and amount of info. sought, reduced accuracy of friend/foe discrimination (Entin & Serfaty, 1990)
    - Decision by fire fighters on when to exit fire: When under high stress, fewer cues were used, had distorted info. processing (Ozel, 2001)

DM: OTHER FACTORS – GROUPS

- Security decisions are often made by groups (e.g., management team, IT dept.)
- An individual's views about risk tend to harmonize with the group he identifies with (Kahan, 2008).
  - Groups tend to polarize.
    - Groups of risk-takers tend to make riskier decisions than the individual members.
    - Groups of cautious people tend to make more cautious decisions than the individual members.

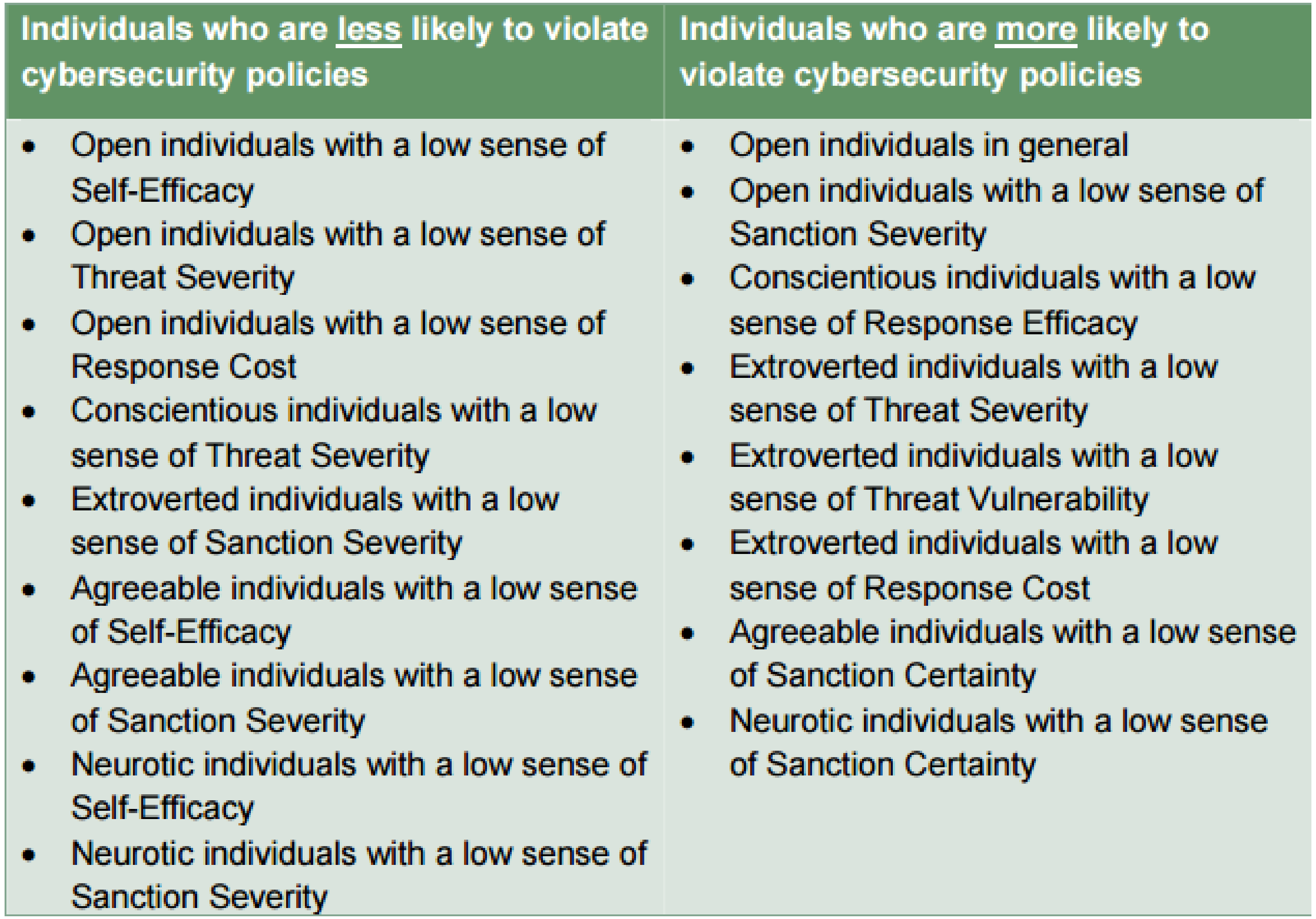
DM: OTHER FACTORS – ORG. ENVIRONMENT

- Examples of factors relating to organizational environment:
  - Self-efficacy (i.e., how capable the person feels about handling the situation)
  - Threat vulnerability (i.e., how vulnerable person feels to threats)
  - Sanction severity (i.e., how much the person thinks s/he will be penalized for security violation)
  - Response efficacy (i.e., how much the person thinks his/her actions matter)

  ➔ These factors can be manipulated through social engineering tactics (e.g., apply time pressure…"Your data will be wiped out in 24 hrs" if you don't pay)

DM: PERSON X SITUATIONAL FACTORS INTERACTING

- Study on Cybersecurity policy violations (McBride, Carter & Warkentin, 2012)



Individuals who are less likely to violate cybersecurity policies	Individuals who are more likely to violate cybersecurity policies
• Open individuals with a low sense of Self-Efficacy • Open individuals with a low sense of Threat Severity • Open individuals with a low sense of Response Cost • Conscientious individuals with a low sense of Threat Severity • Extroverted individuals with a low sense of Sanction Severity • Agreeable individuals with a low sense of Self-Efficacy • Agreeable individuals with a low sense of Sanction Severity • Neurotic individuals with a low sense of Self-Efficacy • Neurotic individuals with a low sense of Sanction Severity	• Open individuals in general • Open individuals with a low sense of Sanction Severity • Conscientious individuals with a low sense of Response Efficacy • Extroverted individuals with a low sense of Threat Severity • Extroverted individuals with a low sense of Threat Vulnerability • Extroverted individuals with a low sense of Response Cost • Agreeable individuals with a low sense of Sanction Certainty • Neurotic individuals with a low sense of Sanction Certainty

DM: THE OTHER GUYS…CYBERATTACKERS

TYPE	WHY? (Motive)	WHO?
National Governments (e.g., Stuxnet, Op. Aurora)	Politically motivated to inflict damage, decrease confidence in critical infrastructure (psychological, economic impact)	Well-funded with lots of resources. Most technologically advanced.
Terrorists (e.g., Pakistani Cyber Army)	Spread terror throughout the civilian population. Political/ideological motives (e.g., cyberattacks to weaken the U.S. economy to detract from the Global War on Terror)	Terror groups.
Industrial spies & Org. crime groups: Insiders & Outsiders (e.g., Target, Sony, Chase)	Money, leverage-able information (trade secrets for blackmail etc.). Use potential public exposure as a threat.	Larger organized groups working slowly and cautiously mimic IT processes to avoid detection.

DM: THE OTHER GUYS…CYBERATTACKERS (CON'T)

TYPE	WHY? (Motive)	WHO?
Hacktivists (e.g., Anonymous, Syrian Electronic Army)	Their goal is to support their political agenda. Their sub-goals are propaganda and causing damage to achieve notoriety for their cause rather than damage to critical infrastructures.	Small groups, usually decentralized and not very organized.
Hackers/Pranksters (e.g., LulzSec)	Fun, entertainment, intellectual challenge.	Usually individuals or small groups. Opportunistic.

These types are not mutually exclusive and can be linked. E.g.,

- Hacktivist who is an insider threat, committing industrial cyber crime.
- Organized crime groups engaging hackers.

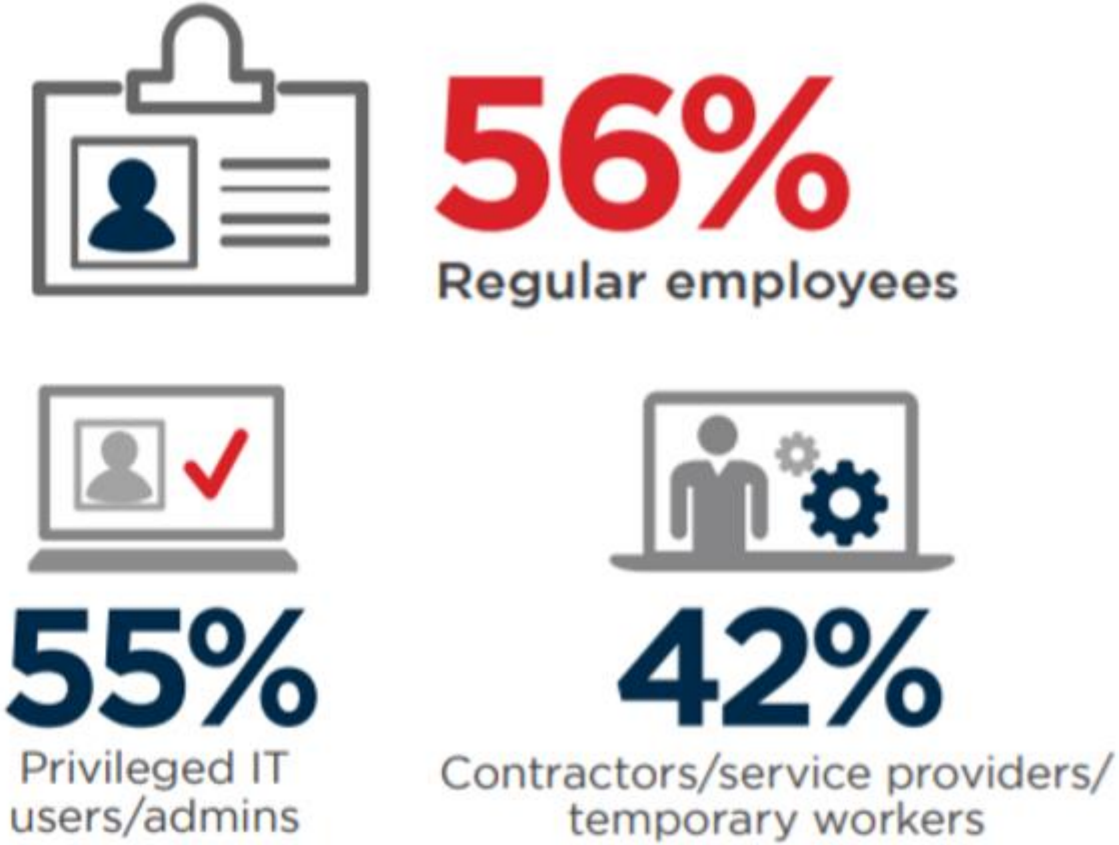
DM: CYBERATTACKERS…INSIDER THREAT

- Insider threat may not be the most common type of threat
  - 1900+ reported incidents in the last 10 years
  - ≈ 19% of incidents involve malicious insider threat actors
- But insider threats are the most costly and damaging
  - Average cost $412K per incident
  - Average victim loss: ≈ $15M / year
  - Multiple incidents exceed $1 Billion
- Insider cyberattackers are only probably the ones we interact with most.

DM: CYBERATTACKERS…INSIDER THREAT

- Insider threats can range from:
  - Careless insider: forgets or neglects to comply with security policies. Non-malicious.
  - Naïve insider: falls prey to social engineering maneuvers. Non-malicious.
  - The Saboteur: disgruntled and want to harm the company for personal gain.
  - Disloyal insider: takes advantage of company for personal gain (e.g., steal intel property, financial/client databases etc.)
  - The Moonlighter: Steals info. to sell to another party (e.g., rival company)
  - The Mole: Been bought out to provide access to company's confidential info.

INSIDERS POSING THE BIGGEST SECURITY RISKS



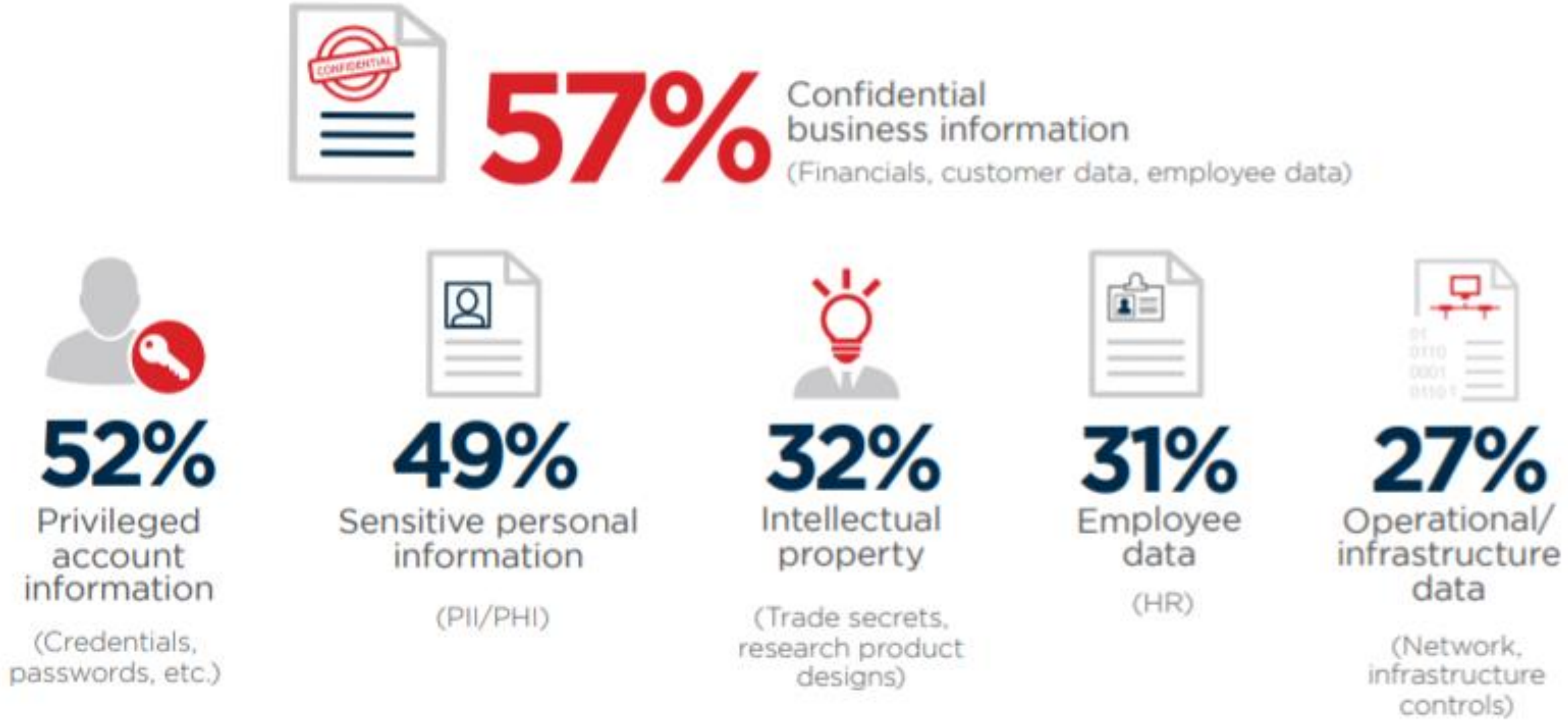
56%
Regular employees

55%
Privileged IT users/admins

42%
Contractors/service providers/ temporary workers

2018 Insider Threat Report - https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf

MOST VULNERABLE DATA



57% Confidential business information (Financials, customer data, employee data)

52% Privileged account information (Credentials, passwords, etc.)

49% Sensitive personal information (PII/PHI)

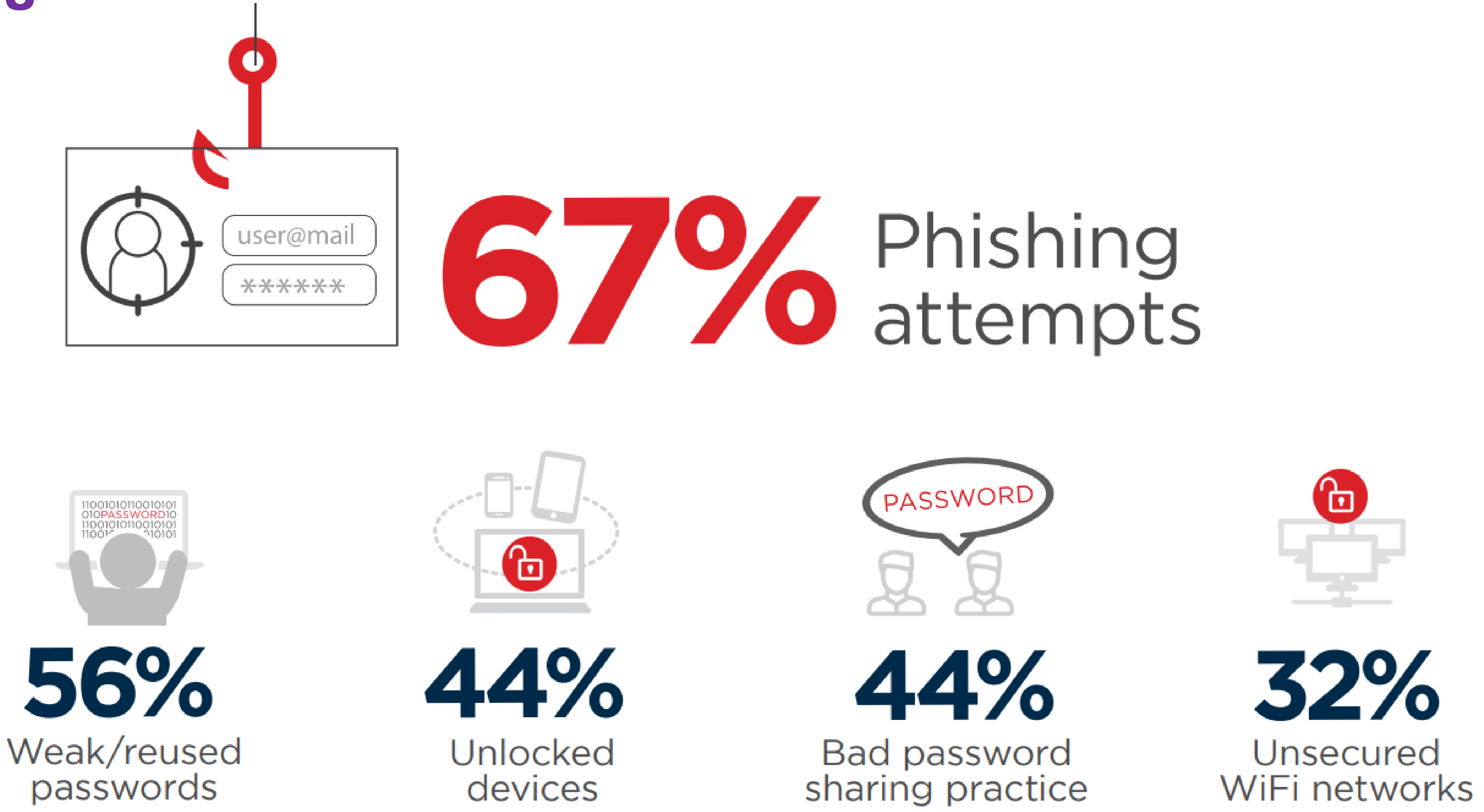
32% Intellectual property (Trade secrets, research product designs)

31% Employee data (HR)

27% Operational/infrastructure data (Network, infrastructure controls)

2018 Insider Threat Report - https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf

Biggest Enabler of Accidental Insider Threats



67% Phishing attempts

56% Weak/reused passwords

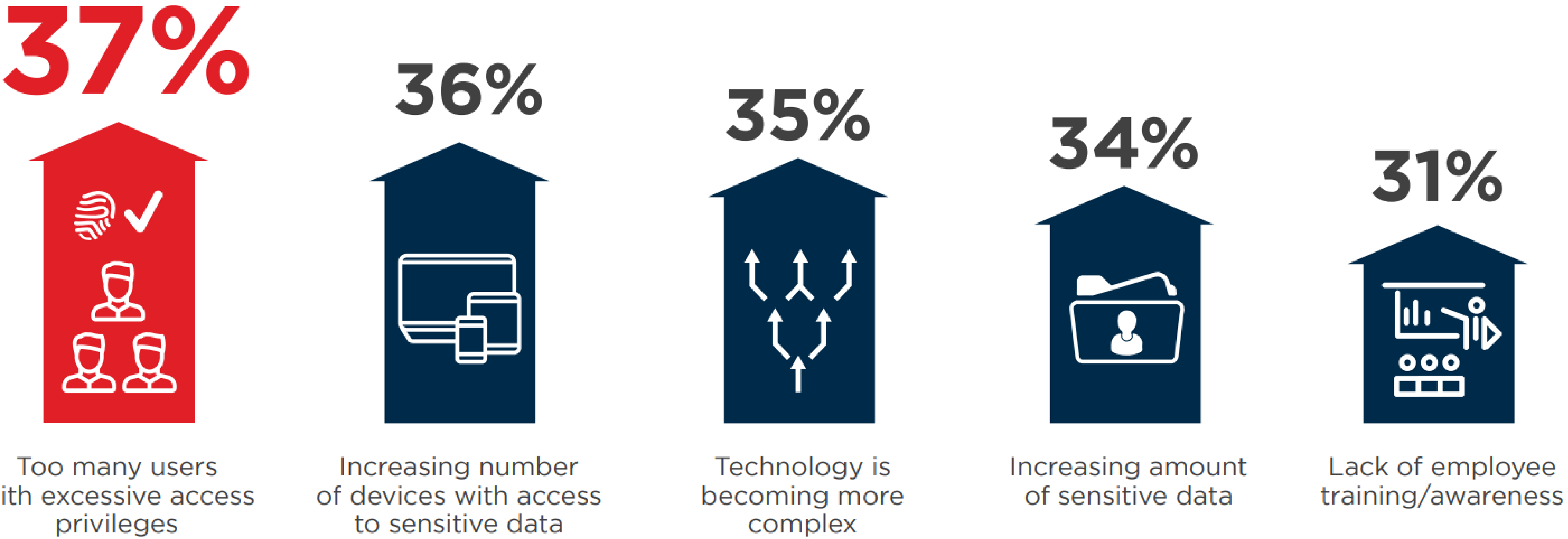
44% Unlocked devices

44% Bad password sharing practice

32% Unsecured WiFi networks

2018 Insider Threat Report - https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf

Main Enablers of Insider Attacks



37%
Too many users with excessive access privileges

36%
Increasing number of devices with access to sensitive data

35%
Technology is becoming more complex

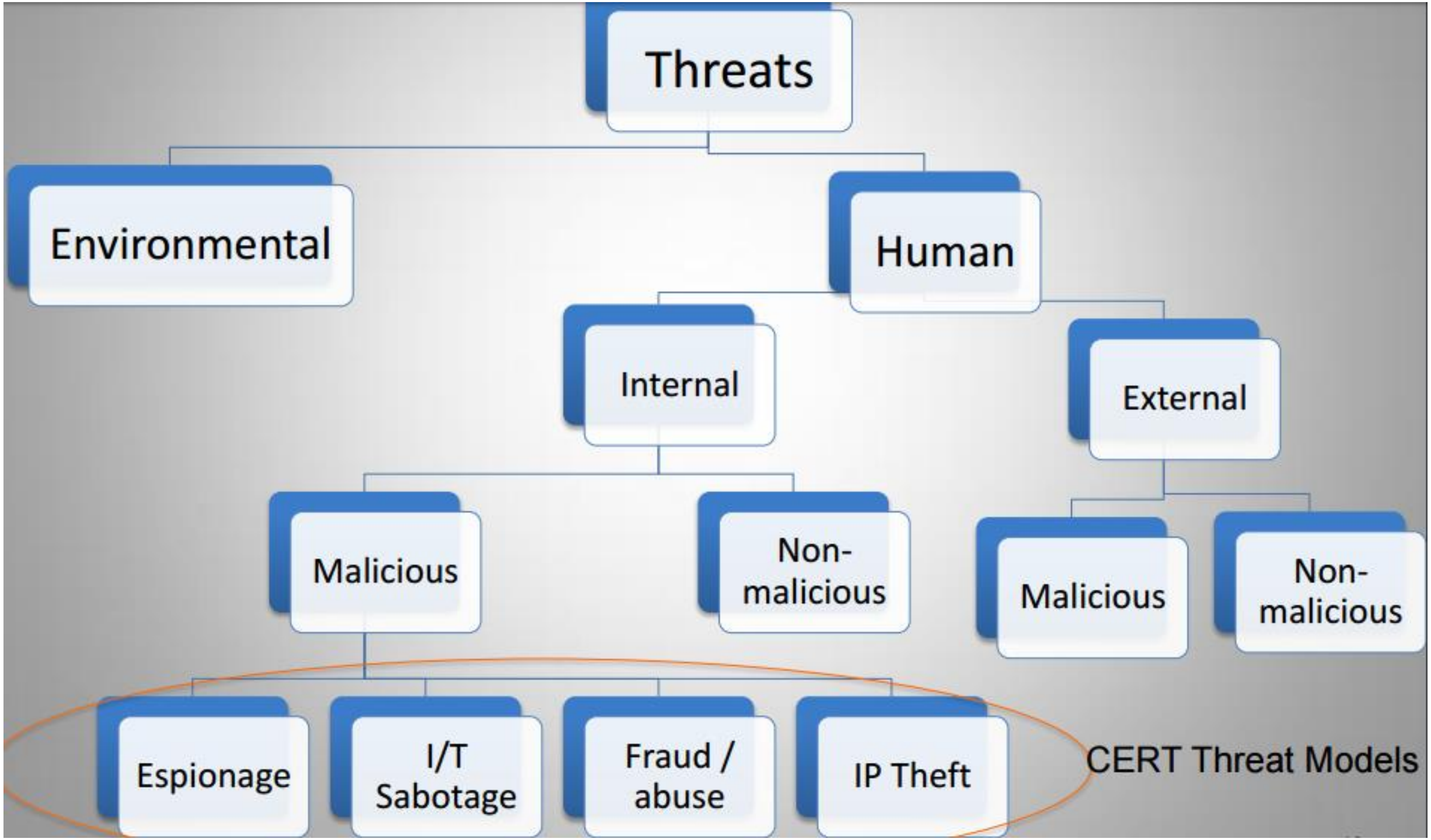
34%
Increasing amount of sensitive data

31%
Lack of employee training/awareness

2018 Insider Threat Report - https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf

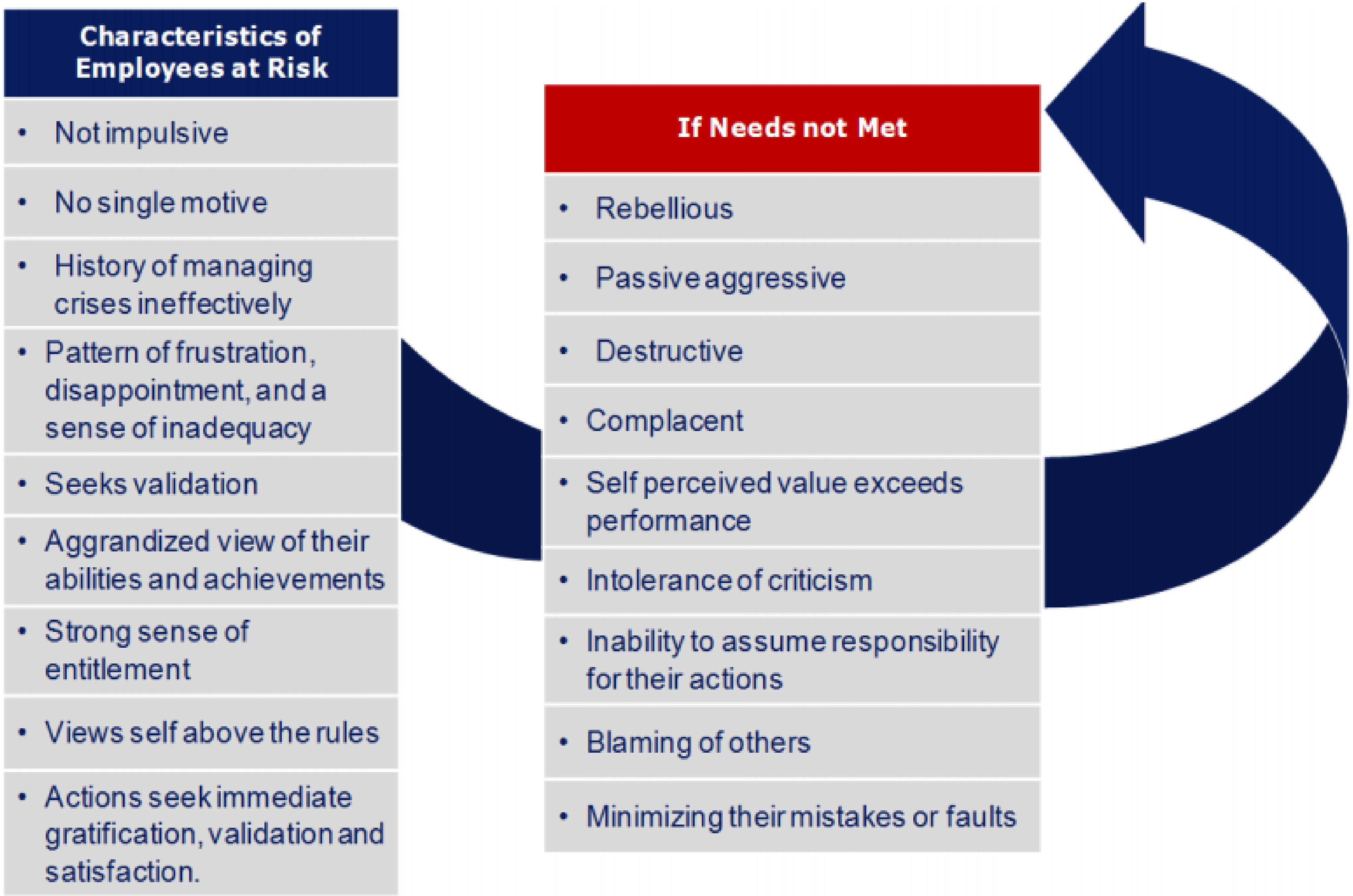
DECISION MAKING: COMMON MISTAKES

- Assume background checks prevent and solve all problems.
  - Can’t know everything about everyone.
  - People change over time, background checks do not really provide measures of an individual’s character, only his or her current state of mind.
- Large amount of security clearances.
  - In 2014, the Office of Management and Budget reported that 5.1 million Americans have security clearances. That is equivalent to 1.5 percent of the population.
  - Have been reduced since then to help prevent insider threats
- Fail to notice Red Flags
- Phishing Attempts


Threats
Environmental
Human
Internal
External
Malicious
Non-malicious
Malicious
Non-malicious
Espionage
I/T Sabotage
Fraud / abuse
IP Theft
CERT Threat Models

DM: CYBERATTACKERS…INSIDER THREAT

- Characteristics of **INSIDERS** at risk of being threats (with malicious intent):



Characteristics of Employees at Risk
Not impulsive
No single motive
History of managing crises ineffectively
Pattern of frustration, disappointment, and a sense of inadequacy
Seeks validation
Aggrandized view of their abilities and achievements
Strong sense of entitlement
Views self above the rules
Actions seek immediate gratification, validation and satisfaction.

If Needs not Met
Rebellious
Passive aggressive
Destructive
Complacent
Self perceived value exceeds performance
Intolerance of criticism
Inability to assume responsibility for their actions
Blaming of others
Minimizing their mistakes or faults

DM: CYBERATTACKERS…INSIDER THREAT

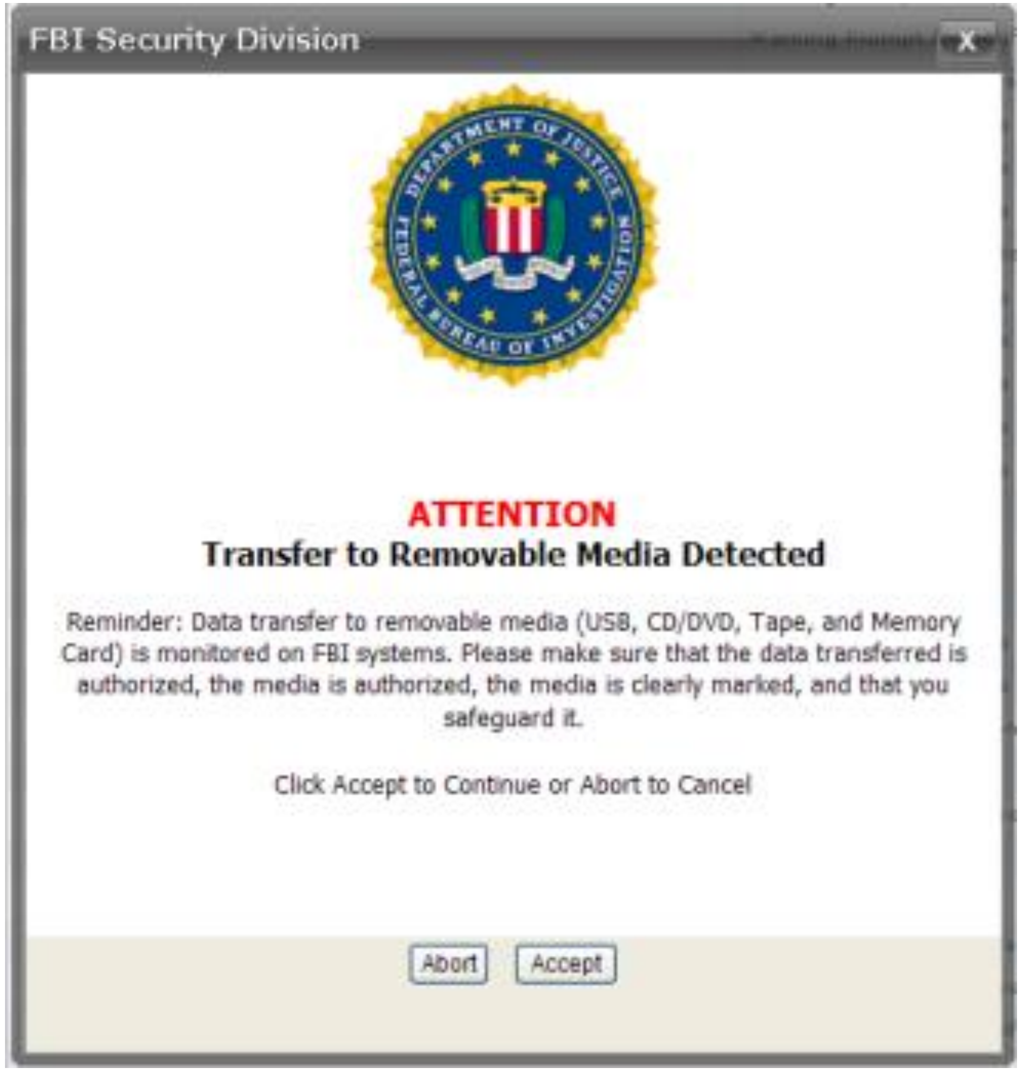
- Behaviors are usually a result of **PERSON X SITUATIONAL** factors interacting (i.e., person factor may predispose, but situation/condition must be "ripe")
- Situational/Organizational factors
  - Availability and ease of obtaining the information/data
  - Have access privileges
  - Classified information not properly labeled
  - Ease of leaving facility with classified info.
  - Undefined policies regarding working on classified projects remotely.
  - Perception of a lax security and minimal consequences for theft.
  - Time pressure
  - Poor training on how to protect classified information.

DM: CYBERATTACKERS…INSIDER THREAT

- **Behavioral indicators of malicious threat activity**
  - Remotely accesses the network while on vacation, sick or at odd times
  - Works odd hours without authorization
  - Notable enthusiasm for overtime, weekend or unusual work schedules
  - Unnecessarily copies material, especially if it is proprietary or classified
  - Interest in matters outside of the scope of their duties
  - Signs of vulnerability, such as drug or alcohol abuse, financial difficulties, gambling, illegal activities, poor mental health or hostile behavior, should trigger concern.
  - Warning signs among employees such as the acquisition of unexpected wealth, unusual foreign travel, irregular work hours or unexpected absences.

DM: CYBERATTACKERS…INSIDER THREAT

- Some measures to deter cyberattackers from inside:
  - Deploy data-centric, not system-centric security (give access to data, not systems)
  - Crowd-source security: share information about threats openly, engage “white hat” hackers
  - Use positive social engineering



ATTENTION

Transfer to Removable Media Detected

Reminder: Data transfer to removable media (USB, CD/DVD, Tape, and Memory Card) is monitored on FBI systems. Please make sure that the data transferred is authorized, the media is authorized, the media is clearly marked, and that you safeguard it.

Click Accept to Continue or Abort to Cancel

DM: CYBERATTACKERS…INSIDER THREAT

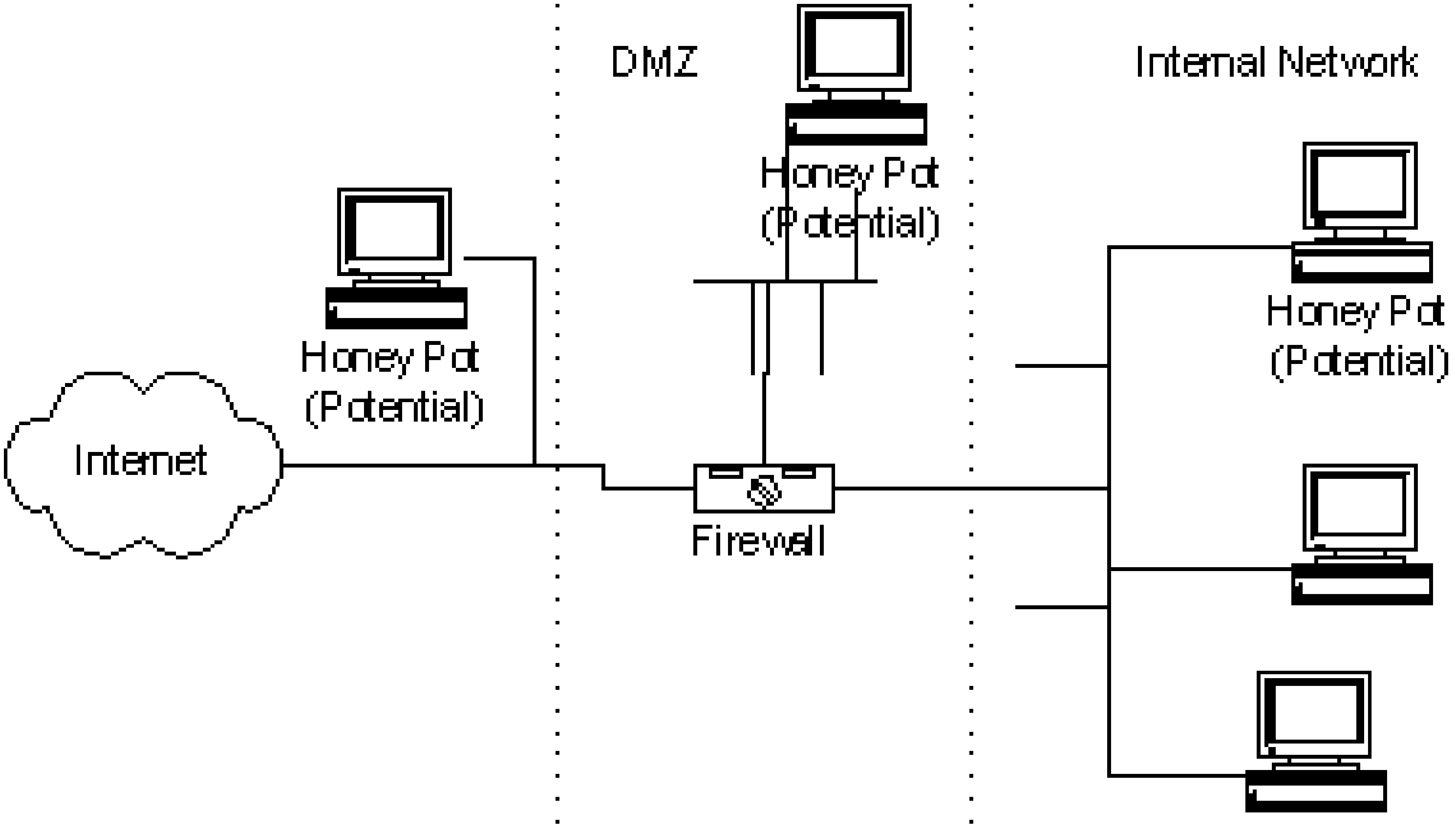
- **Some measures to deter cyberattackers from inside (con't):**
  - Hard to trawl through large volume of data to find insider. Can't know everything about everyone.
    - May not be feasible to predict who is going to be insider threat.
    - Look out risk factors among personnel and zoom in (Person X Situation vulnerabilities).
      - Build a baseline of user's volume, velocity, frequency, amount of network traffic based on hourly, weekly, monthly patterns of at-risk personnel
  - Require identification for all assets (passwords, access cards)
  - Note frequent visits to sites
  - Announce use of policies that monitor events like unusual network traffic spikes, volume of USB/mobile storage devices, volume of off-hour activities, inappropriate use of encryption…

DM: CYBERATTACKERS…THE OTHER THREATS

- Can’t monitor decisions/activity until they strike.
- Use tools and framework for understanding their DM.
- Underscores importance of having cyber-resilient systems (i.e., system design)

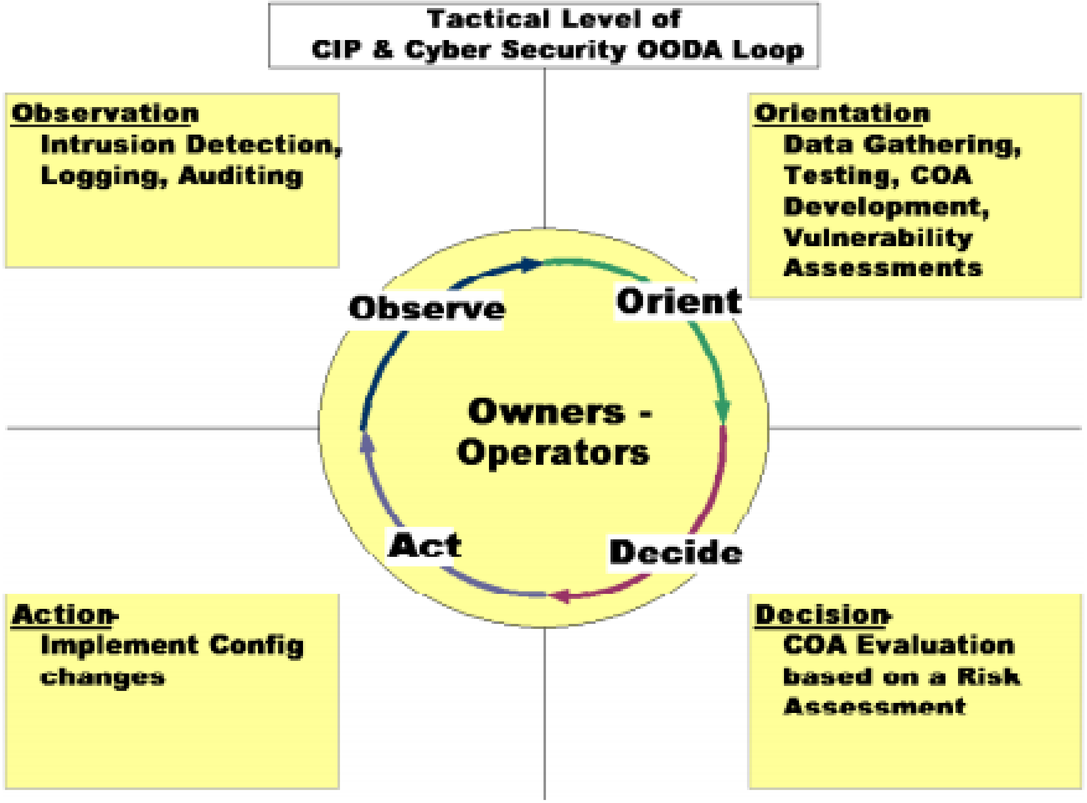
TOOLS FOR UNDERSTANDING CYBERATTACKERS' MO

- Honeypots: dummy system on network containing misleading/false content to lure attackers in order to observe his tactics and distract him from the real system.
  - Emulate real operating systems/servers, but not in the same location as the real network (e.g., DMZ that buffers the LAN from outside internet)
  - Can give early warning of an attack
  - Can collect attacker's IP address and other info.
  - Research Honeypots : collect info. on cyber threats via log files etc.
  - Production Honeypots : used to protect organizations
    - Can slow down attacker's scanning tools (waste time), stop attacks



Potential locations for honeypots

FRAMEWORK FOR UNDERSTANDING DM : OBSERVE-ORIENT-DECIDE-ACT (OODA) LOOP



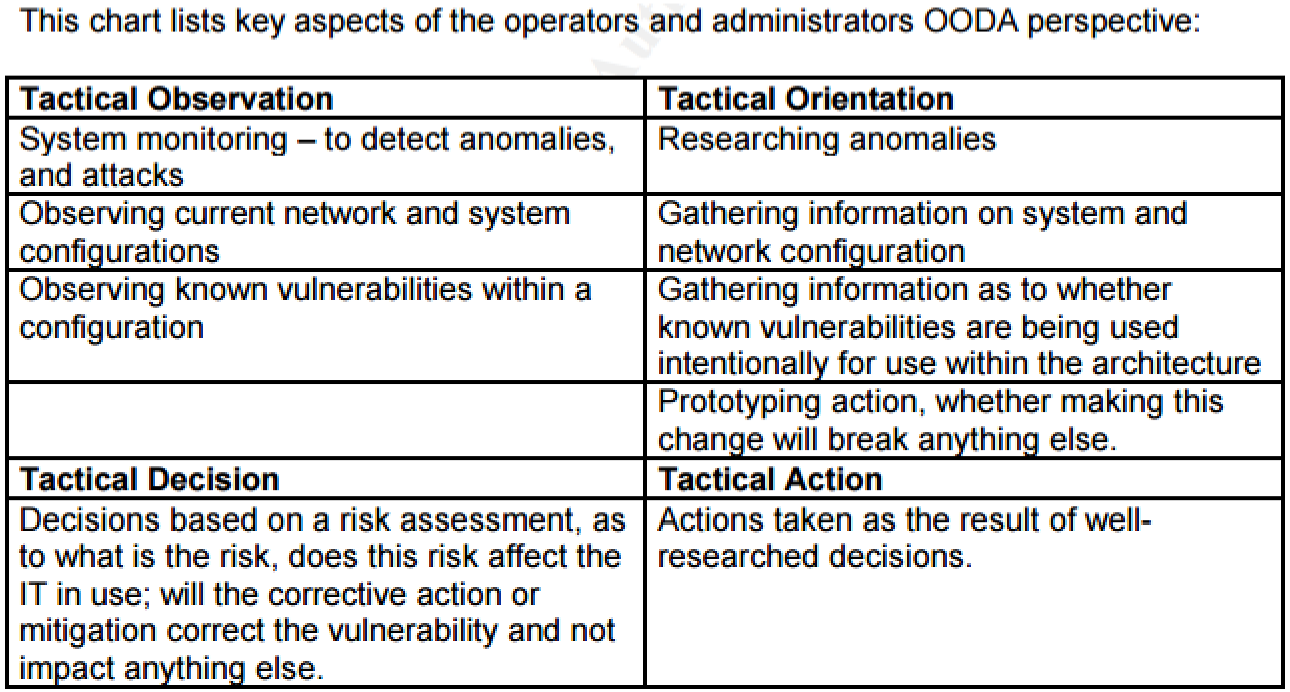
Tactical Level of CIP & Cyber Security OODA Loop

Observation
Intrusion Detection, Logging, Auditing

Orientation
Data Gathering, Testing, COA Development, Vulnerability Assessments

Action
Implement Config changes

Decision
COA Evaluation based on a Risk Assessment



This chart lists key aspects of the operators and administrators OODA perspective:

Tactical Observation	Tactical Orientation
System monitoring – to detect anomalies, and attacks	Researching anomalies
Observing current network and system configurations	Gathering information on system and network configuration
Observing known vulnerabilities within a configuration	Gathering information as to whether known vulnerabilities are being used intentionally for use within the architecture
	Prototyping action, whether making this change will break anything else.
Tactical Decision	**Tactical Action**
Decisions based on a risk assessment, as to what is the risk, does this risk affect the IT in use; will the corrective action or mitigation correct the vulnerability and not impact anything else.	Actions taken as the result of well-researched decisions.

CYBER PREVENTION TRENDS

- Organizations are shifting their focus on detection of insider threats (64%), followed by deterrence methods (58%) and analysis and post breach forensics (49%).
- The use of user behavior monitoring is accelerating; 94% of organizations deploy some method of monitoring users and 93% monitor access to sensitive data.
- The vast majority (86%) of organizations already have or are building an insider threat program. Thirty-six percent have a formal program in place to respond to insider attacks, while 50% are focused on developing their program.

AREAS TO WORK ON

1. **Improve security awareness among information infrastructure builders.**
   - Usability (esp. since security is not the primary task of users)
     - Assign trust score to each document that reflects trustworthiness of content and content provider? Balance security with performance and usability, do not want unwieldly policies

2. **Enhance situational awareness during cyber attacks**
   - Trustworthiness of information from primary sources (i.e., system sensors, network activity) and secondary sources (i.e., other people, automated interpretation of events)

3. **Supporting decisions about trustworthiness of network transactions**
   - How much can the relevant information be trusted?
   - Visibility of important information at the correct time
   - Accuracy of analysis (reduce faulty assumptions)

Insider Threats Recap

- Are uncommon but have the largest impacts
- Common mistakes lead to accidental insider threats
- Can be minimized with proper awareness and training