



MIDWEST
RELIABILITY
ORGANIZATION

2022 Annual Security Insider Threat Training

October 4, 2022

CLARITY

ASSURANCE

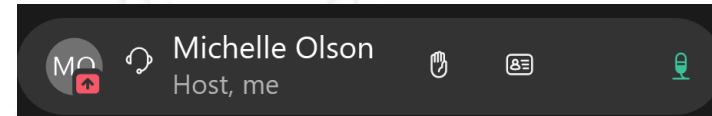
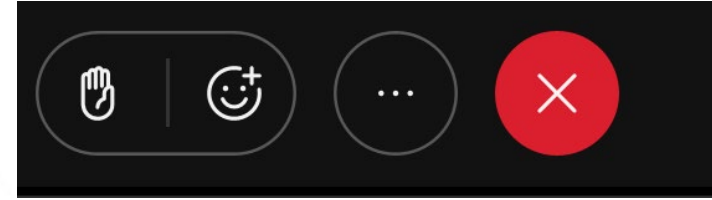
RESULTS

WebEx Chat Feature

Please hold questions until the end of each presentation unless speakers recommend otherwise.

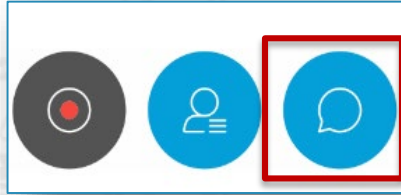
If you would like to verbally ask your questions, please use the raise hand feature and we will unmute you.

If you would like to submit questions as the speakers are presenting, please submit them via the chat.



WebEx Chat Feature

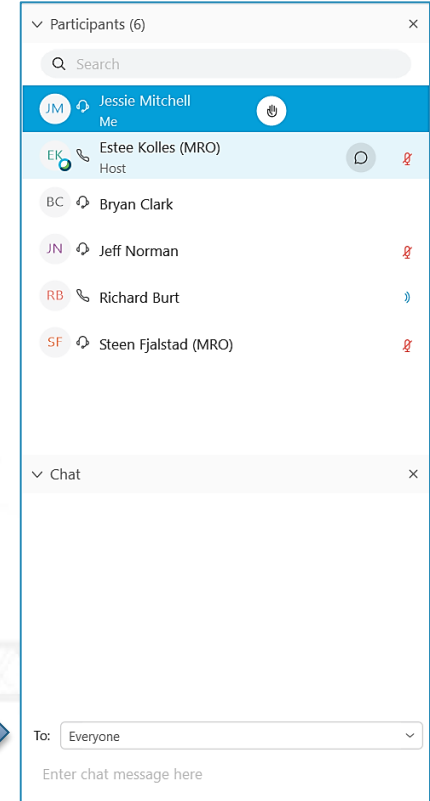
Open the Chat Feature:



The chat feature will appear to the right of the WebEx window.

Attendees should chat their questions to: “MRO Host”.

Select MRO Host by using the drop down arrow in the “To” field.



CLARITY

ASSURANCE

RESULTS

Disclaimer

The Midwest Reliability Organization (MRO) Security Advisory Council (SAC) is committed to providing training and non-binding guidance to industry stakeholders regarding existing and emerging security topics. Subject Matter Experts (SMEs) developed any materials, including presentations, through the MRO SAC from member organizations within the MRO Region and other government and industry security experts. The views in this presentation are presented by these MRO SAC SMEs, government, and industry experts, and do not express the opinions and views of MRO.





MRO 2022 Regional Risk Assessment

Top risks to the reliable and secure operation of the North American bulk power system in MRO's regional footprint.

Top Reliability Risks

Uncertainty of Winter Planning Reserve Margins

Analyses of recent system events indicate that actual system conditions can and have exceeded forecast winter reserve margins, particularly during cold weather conditions in the south central U.S.

Generation Availability During Severe Cold Weather

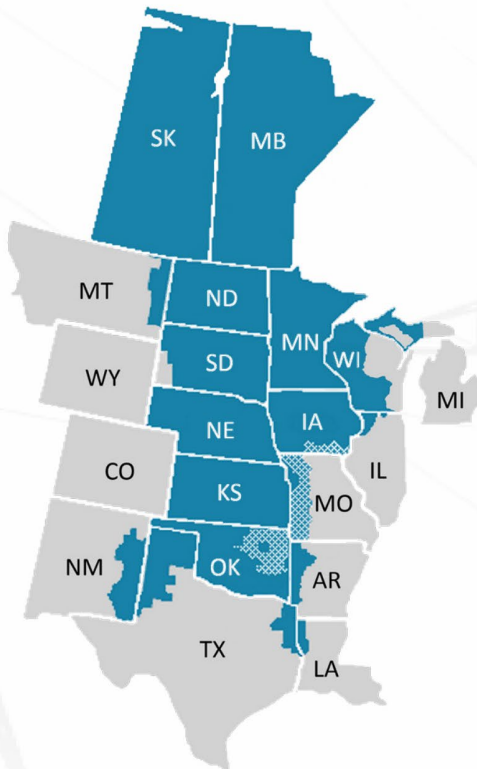
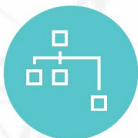
Generation availability assumed during cold weather in the southern U.S. has been shown to be unrealistically high due to a lack of generator winterization and natural gas curtailments.

Lack of Energy Assurance Assessments

The rapidly changing resource mix requires rethinking the way in which generating capacity, energy supply, and load serving needs are studied. Energy assurance will need to be accurately assessed for all hours of the year with increasing reliance on wind and solar as a fuel source.

Bulk Power System Modeling Accuracy

The rapid increase in inverter-based resources, along with the changing characteristics and magnitude of load related to distributed energy resources (DER), is challenging current bulk power models.



Top Security Risks

Supply Chain Compromise

The risk of a cybersecurity event carried out through the vendor supply chain and possibly impacting reliability of the bulk power system remains high.

Insider Threats

The threat of an employee or a contractor using authorized access, wittingly or unwittingly, to do harm to the security of the bulk power system has increased given remote connectivity during the pandemic.

Malware and/or Ransomware

Vulnerability to a malware and/or ransomware attack on the bulk power system continues to increase with modernization and the deployment of new technologies.



More information on these risks along with mitigation recommendations can be found in the full report here: www.mro.net

MRO Security Risk Priorities for 2022

MRO Reliability Risk Matrix - Physical and Cyber Security Risk Rankings						
Consequence/Impact (C)		Likelihood (L)				
		L1	L2	L3	L4	L5
		Very Unlikely	Unlikely	Possible	Likely	Almost Certain
C5	Severe					
C4	Major				7	
C3	Moderate			4 5		
C2	Minor		1 6	2 3 8 9 11		
C1	Negligible			10		

	Physical and Cyber Security Risks
1	Inability to Access and/or Apply Threat Intelligence - New
2	Inadequate Resources *
3	Focus on CIP Compliance *
4	Insider Threat *
5	Malware/Ransomware - New
6	Security Awareness & Training - New
7	Supply Chain Compromise *
8	Vulnerability & Support Challenges of Legacy Devices *
9	Asset Inventory & Management - New
10	Network Visibility & Monitoring - New
11	Perimeter Security & Controls - New

The three risks in the orange section of the security risk heat chart have been identified as having the highest relative risk and are:

- Supply Chain Compromise
- Insider Threat
- Malware/Ransomware



AGENDA

Tuesday, October 4, 2022 | 8:00 a.m. to 4:30 p.m. Central

8:00 a.m. – 9:00 a.m.	Breakfast & Networking
9:00 a.m. – 9:10 a.m.	Training Welcome <i>Steen Fjalstad, Director of Security, MRO</i>
9:10 a.m. – 10:10 a.m.	Industry Insider Threat Program Expert <i>Keith Jones, Director of Security, RWE Americas Inc.</i>
10:10 a.m. – 10:30 a.m.	Morning Break
10:30 a.m. – 11:30 a.m.	Industry Insider Threat Program Expert <i>Keith Jones, Director of Security, RWE Americas Inc.</i>
11:30 a.m. – 12:30 p.m.	Lunch & Networking
12:30 p.m. – 2:30 p.m.	Employee Mental Health and Insider Threat Connections <i>Dr. Rosie Ward, CEO and Co-Founder, Salveo Partners, LLC</i>
2:30 p.m. – 2:50 p.m.	Afternoon Break
2:50 p.m. – 4:20 p.m.	Focusing on Active Shooter <i>Trooper Tod L. Hileman, Kansas Highway Patrol</i>
4:20 p.m. – 4:30 p.m.	Wrap up and Questions <i>Steen Fjalstad, Director of Security, MRO</i>





**Developing an
Insider Threat Identification
And Mitigation Program**

Presented by:

Keith Jones

October 4, 2022

Overview

Developing an ITIMP

- Why create and ITIMP
- Program Development Process
- Minimum Standard Requirements
- Roles and Responsibilities
 - Working Group
 - Individual Members of the Working Group
- Program Approval Process
- Program Roll Out
- Case Management System
- Question and Answer Session

Alignment

- This briefing is based on the National Security mandated Insider Threat Program
- Actual references to the National Security Program requirements are provided for your examination and contemplation
- Currently there is no requirement for the energy sector to implement an Insider Threat Program

Definition - Insider Threat

- An insider threat is an event where a current or ex; employee, consultant, business partner, vendor, or other third party wittingly or unwittingly create risk
- Risk includes exposing people, information, property, and company reputation to undesirable risk that can result in injury or death, damage to property, compromise of intellectual property, financial loss, and reputational harm.

Why Create an Insider Threat Program?

- Identified as a high risk by security professionals in the energy sector (MRO and State of Texas)
- Impactful (I have empirical data) about mitigating risk
- Required by Executive Order in some industries
- Invest in your people and company; **statistics about helping**
- It will create or enhance a culture of Security Awareness

Examples - Insider Threat

- Data loss via phishing, spear phishing, Ransomware
- Ignorance of or failure to follow company policy, no policy in place; **SPLUNK example**
- Theft of Trade Secrets, lack of adequate protection for Trade Secrets
- Piggybacking into work buildings/sensitive areas; **PEN testing example**
- Misuse of information technology systems
- Defeating security controls on computers
- Account and password sharing
- Taking IT devices or proprietary information outside of the U.S.
- Whenever people do not comply with company policy; Insider Threat

Specific Examples - Insider Threat

- Credited with saving the life of a suicidal employee
- Responsible for identifying many spies attempting to commit espionage
- Enhanced company policy (many times)
- Empowers (by policy) employees to “See Something Say Something”
- Created a “Swarm Intelligence” approach to risk management; **9/11 example**

Result:

- Created a culture of Security Awareness

EO 13587 - Requirements



- Establish a program for deterring, detecting, and mitigating insider threats
- Establish a centralized capability to monitor, audit, gather, and analyze information
- Develop and implement sharing policies and procedures whereby collected information is shared across the organization
- Designate a Senior Official with authority to provide management, accountability, and oversight
- Consult with records management, legal counsel, civil liberties and privacy officials
- Obtain additional department/agency guidance if needed
- Perform self-assessments for compliance
 - Report results to Senior Official and Working Group and Board Members
- Enable independent assessments

Program Development Process

Step 1 – Identify the Team

- Senior Official
- Security
- Human Resources
- Employee Assistance Program (EAP)
- Information Technology
- Legal
- Audit
- Ethics
- Communications
- Operations
- Outside resources as required
- Law Enforcement



Setting Up an Insider Threat Program

Roles and Responsibilities

Personnel Information

- Security
- EAP
- Human Resources
- Audit
- Ethics

Legal Guidance

- General Counsel

System Monitoring

- Information Technology
- Information Assurance

Working Group
Establishes Program



Program Development Process

- What is most critical?
- How sensitive is it?

Step 2 – Conduct a Risk Assessment

- Is it protected? What is the risk if it was leaked?
- Would its loss disrupt time-sensitive processes?
- Would its compromise or degrade company strategy?
- If unaddressed can personal conduct escalate or cause harm?
- Would it help an adversary gain advantage?
- Who has access to the information or where is the information?
 - Should access be changed?
- May include people, facilities,, technology and/or equipment, proprietary information, warehouses
- Risk assessment revealed: **SPLUNK Travel Initiative / “Reward if Returned” program**



Program Development Process

Step 3 – Review & Refine Procedures

- Update rules / company handbook
- Graduated scale of disciplinary action policy
- Document expectations to employees and contractors
- Track acknowledgement
- Ongoing Training & Awareness campaign; **CEO**



Program Development Process

Step 4 – Training

- Incorporate Insider Threat Into Annual Refresher Training
- Provide policy updates real-time
- Track training/acknowledgement (to be legally defensible), annually
- Make it easy for team to report confidentially
 - Anonymous Internal Hotline Number/Email



Implementing the Plan



Information Sources

- Security
- Human Resources
- Audit
- Legal
- Information Technology
- Law Enforcement

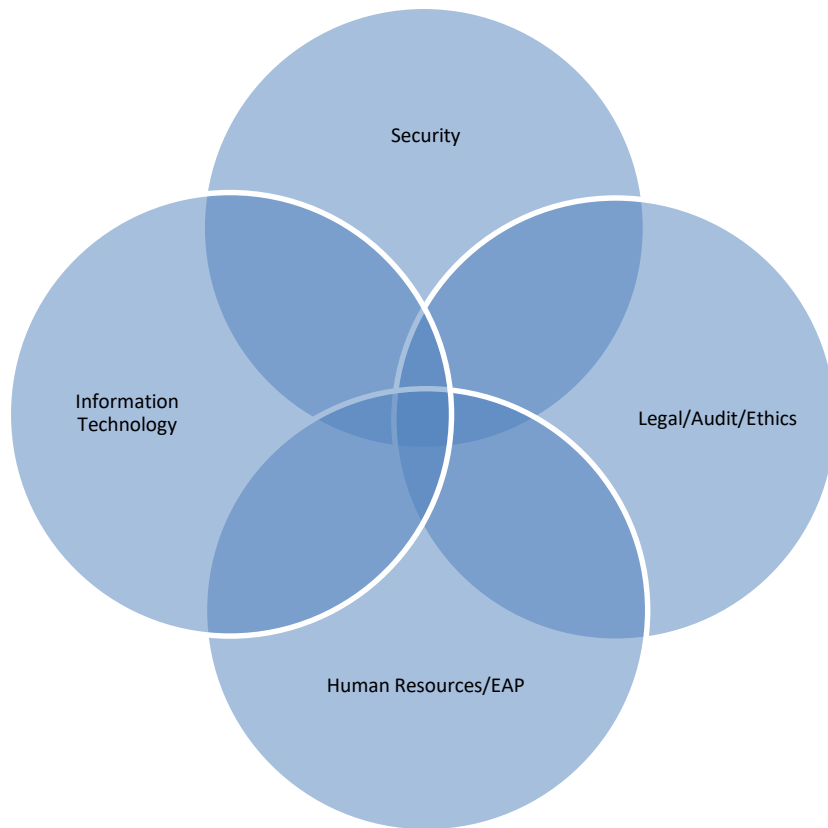
Response Procedures

- Incident response actions

Documentation Includes

- Tracking / Trends; Improvement

Keys to Success

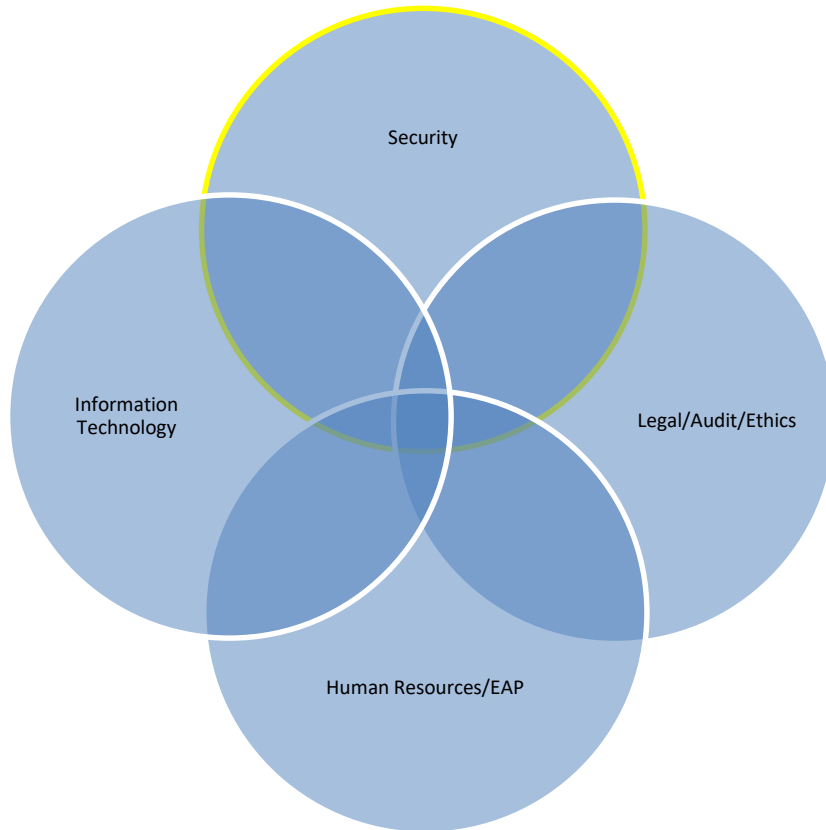


Information Collection

A Comprehensive Insider Threat Program will collect information from multiple sources

- Security
- Information Technology
- Audit
- Legal
- Human Resources
- EAP
- Audit/Ethics

Information Collection

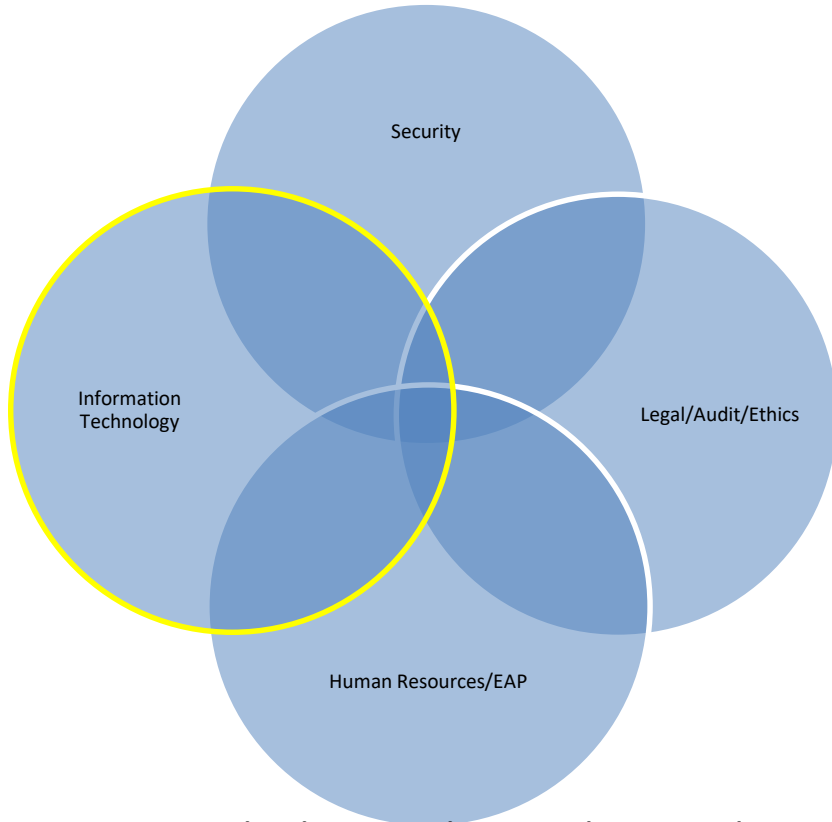


Security

- Facility Access Records
- Garnishments
- Security Incident Reports
- Internal / External Reporting
- Foreign Travel
- Foreign Contacts
- Background Investigation
- Adverse Information

Information Collection

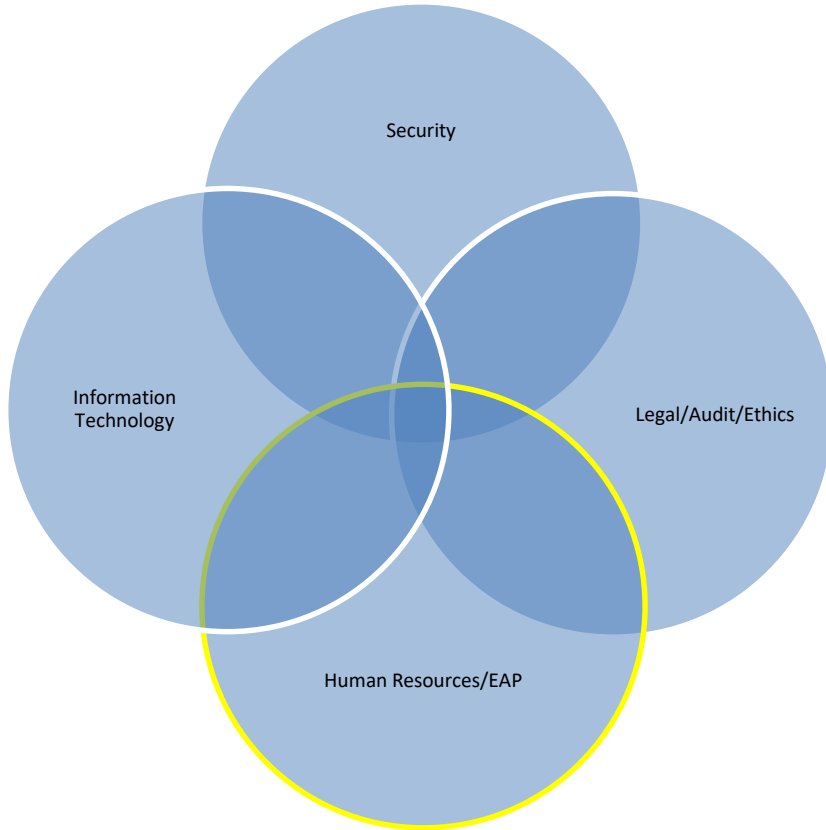
Information Technology



- Cloud storage outside of policy
- Unauthorized software installations
- Levels of network access
- Unsuccessful access attempts
- Adding unauthorized peripherals
- Email transmissions/receipt
- Defeating security controls
- Accessing prohibited websites

Minimum Standard: Promulgate policies and procedures for system and user activity monitoring

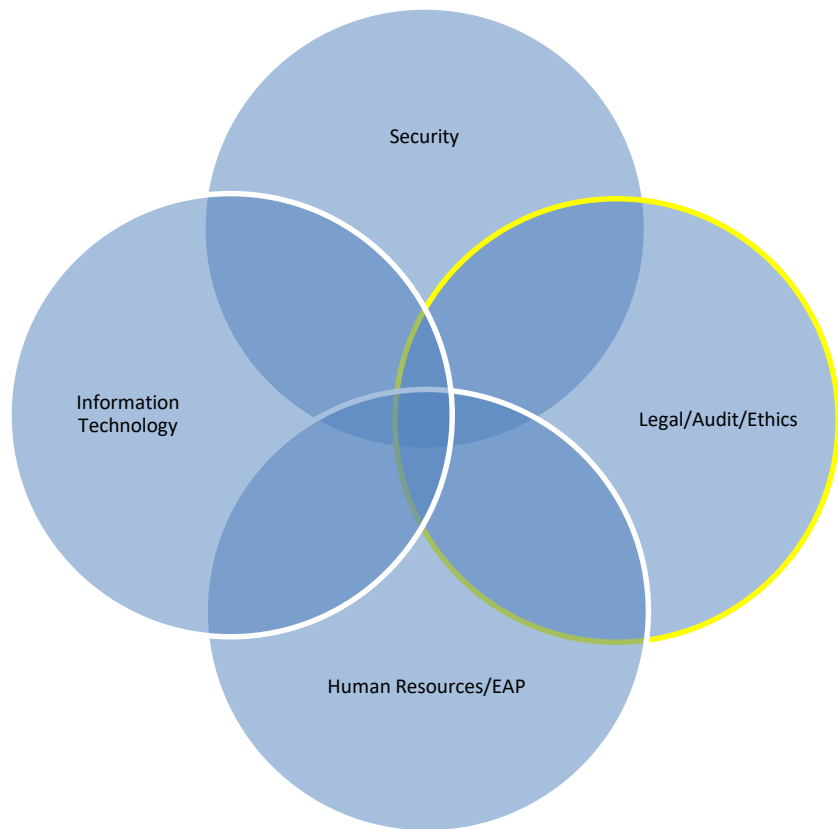
Information Collection



Human Resources

- Performance concerns
- Disciplinary action
- Absenteeism
- Timecard anomalies
- Inappropriate behavior
- Anomalous behavior
- Work abandonment

Information Collection



Legal/Audit/Ethics

- Legalities of program

- Audit & Ethics

Investigations

- Fraud, Waste & Abuse
- Civil Liberties & Privacy

Employee Assistance Program

- Must be a business partner whether in-house or outsourced
- EAP has been an indispensable resource to me and referred employees
- Reach out to EAP now and establish a relationship prior to an event
- Consider making the initial appointment with EAP for employees who are acting in a questionable or unacceptable manner
- You can mandate counseling at the juncture of a terminable offense

Personnel Training Required

Insider Threat Working Group



Fundamentals of Company Policies and Procedures



Conducting Insider Threat Response Actions



Records & Data / Applicable Laws & Regulations



Civil Liberties & Privacy / Laws, Regulations, Policies



Reporting Requirements

Personnel Training Required

Insider Threat Working Group



Security Training Education Professionalization Portal



Insider Threat Awareness (CI121.06)



Establishing and Insider Threat Program for your Organization (CI122.06)



Integrating CI and Threat Awareness into Your Security Program (CI010.16)



NISP Reporting Requirements (IS150.16)

Personnel Training Required



Current and Potential Threats



Detecting and Reporting



Recruitment and Information Collection Methodologies



Behavior Indicators and Reporting Procedures



Counterintelligence and Security Reporting Procedures

Minimum Standard

- Personnel must complete training within 30 days of hire or requirement to access classified information
- Annual refresher training

Personnel Training Required



Information Required to be Contained Within Classified Channels



Tracked Acknowledgement



Web portal with Insider Threat Information, Reporting Requirements,
Threat Trends Analysis

Additional Resources

- Company Website
 - Security / Insider Threat
 - ITIMP Handbook
 - ITIMP Slide Presentation / Training
 - Counterintelligence Brochure
 - Insider Threat Brochure
 - Reporting the Threat Brochure
 - 2014 Trend Analysis / Targeting U.S. Technologies Report
 - Target Technologies and Information Flier
 - Team Member Reporting Requirements Flier



Reporting Channels

- Employee Hotline 1-888-215-1777
- Anonymous Email www.ethicspoint.com
- DoD Hotline 1-800-424-9098 (Toll-Free)
- Case Management



Unclassified Log-In Banner

>> FOR OFFICIAL PURPOSES ONLY <<

All activity on this network is monitored for lawful U.S. Government and authorized purposes. Misuse of this network or network devices for unauthorized purposes can result in criminal and or administrative actions against users.

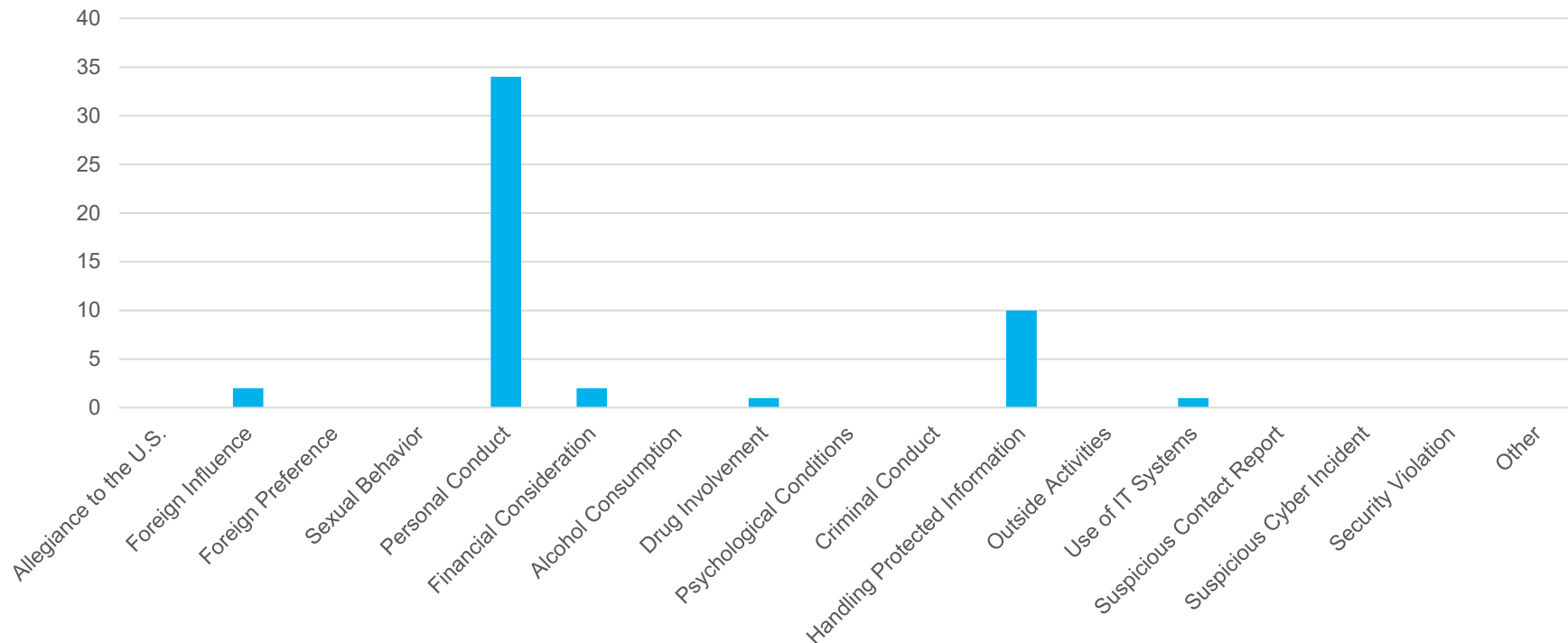
Lock your system (Ctrl Alt Delete) when left unattended.

Click OK to indicate your acceptance of this information.

Excel Spreadsheet: Tracking System

	Date of Incident	Name	Inquiry Official Initials	Explanation of Incident	Cleared	HR	IT	Legal	Security	Audit	Allegiance to the U.S.	Disposition	Notes
1	11/29/16		EG	Theft	No	No	No	No	Yes	No	Personal Conduct	Disciplinary Action Administered	Terminated
2	12/6/16		KJ	Improper use of Draper IP	Yes	No	No	No	Yes	No	Personal Conduct	Adverse Information Report Sent	MIT LL sent report
3	12/8/16		PT	Shared computer access	Yes	No	No	No	Yes	No	Use of IT Systems	No Adverse Information Report Sent	Counseled/Rebriefed
4	12/29/16		KJ	Notice of levy	No	No	No	No	Yes	No	Financial Consideration	No Adverse Information Report Sent	Adverse previously sent
5	12/13/16		KJ	Deliberate disregard of company rules	Yes	No	No	No	Yes	No	Personal Conduct	Adverse Information Report Sent	Terminated
6	12/14/16		TR	Unauthorized trusted download	Yes	No	No	No	Yes	No	Handling Protected Information	No Adverse Information Report Sent	Counseled/Rebriefed
7	12/19/16		KC	Classified paper left out	Yes	No	No	No	Yes	No	Handling Protected Information	No Adverse Information Report Sent	Counseled/Rebriefed
8	12/20/16		CO	Over classification	Yes	No	No	No	Yes	No	Handling Protected Information	No Adverse Information Report Sent	Counseled/Rebriefed
9	1/3/17		KJ	Income withholding for support order	Yes	No	No	No	Yes	No	Financial Consideration	No Adverse Information Report Sent	Counseled/Rebriefed
10	1/6/17		PT	Unlocked workstation	Yes	No	No	No	Yes	No	Handling Protected Information	No Adverse Information Report Sent	Counseled/Rebriefed
11	1/6/17		LM	LAN Contamination	Yes	No	No	No	Yes	No	Handling Protected Information	No Adverse Information Report Sent	Counseled/Rebriefed
12	1/9/17		EG	open container violation	Yes	No	No	No	Yes	No	Personal Conduct	No Adverse Information Report Sent	Counseled/Rebriefed
13	1/9/17		EG	Unlocked safe	Yes	No	No	No	Yes	No	Handling Protected Information	No Adverse Information Report Sent	Counseled/Rebriefed

Tracking System



Summary: Incident Response

- Incident team convenes based on seriousness of report/incident, immediately; best to have an emergency communication channel: **Boston Marathon Bombing**
- Coalesce all available information (HR good starting point)
- Evaluate information available and act soonest
- Bring in needed resources (manager/expertise)
- Notify others who might be a target
- Swarm Intelligence and swift address is key
- Conduct lessons-learned after each incident
- Update policies/procedures/rules/regulations, etc., as needed/required; retrain people
- Track threat trend analysis and improve overall risk posture
- Finally: I will demonstrate an actual Incident Response by sharing a story with you that saved an employee's life...



Open Discussion

Keith Jones, Director, Security - RWE - Americas

773-551-0607

Keith.Jones@RWE.com

Creating Fearless, Emotionally Agile Workplaces

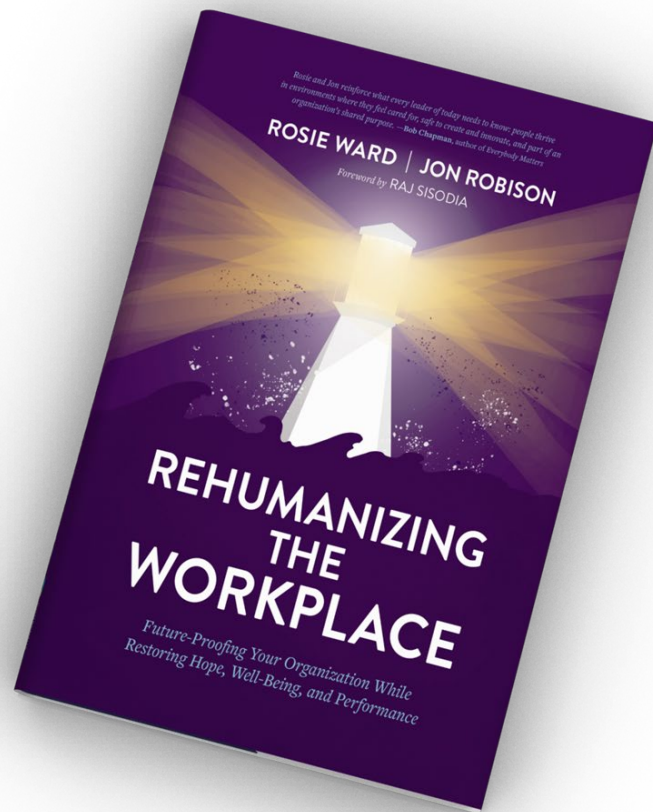
Rosie Ward, Ph.D., MPH, MCHES, BCC, CIC®



***What's the future of leadership; who
will still be standing in 5 years?***

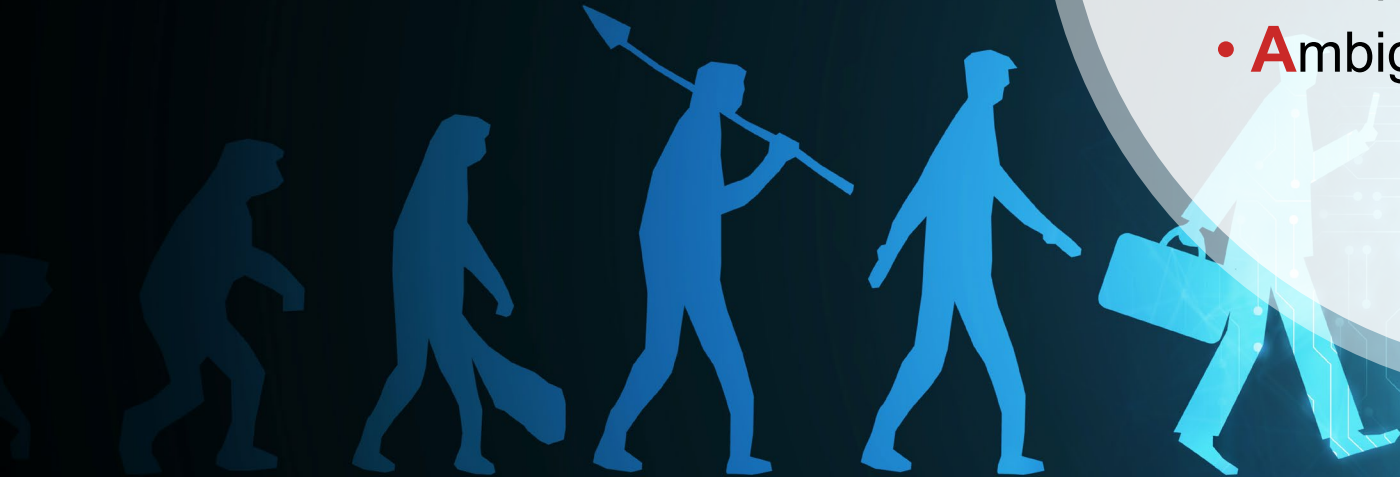
**We need braver leaders and
courageous cultures**

“Leadership is **maximizing our positive impact on the world** by **becoming our best, fully authentic selves** and supporting those around us to break past barriers and step into their greatness.”



Our New Disruptive Reality...

- **V**olatile
- **U**ncertain
- **C**omplex
- **A**mbiguous





**Uncertainty
Risk
Emotional Exposure**

Armoring Up

SHAME
SCARCITY
FEAR
ANXIETY
UNCERTAINTY





LOVE
BELONGING
JOY

SHAME
SCARCITY
FEAR
ANXIETY
UNCERTAINTY





COURAGE
EMPATHY
TRUST
INNOVATION
CREATIVITY
ACCOUNTABILITY
ADAPTABILITY
INCLUSIVITY | EQUITY
HARD CONVERSATIONS
FEEDBACK
PROBLEM-SOLVING
ETHICAL DECISION MAKING
RESILIENCE | RESETTING

LOVE
BELONGING
JOY

SHAME
SCARCITY
FEAR
ANXIETY
UNCERTAINTY









We the People of the United States
In order to form a more perfect Union, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do hereby ordain and establish this Constitution for the United States of America.

Article 1

Section 1

Roe v. Wade



Trauma Response

Over-Functioners

Under-Functioners



*Today's average employee can absorb
half as much change as they could
manage in 2019*



FOR IMMEDIATE RELEASE

December 7, 2021

Contact: HHS Press Office

202-690-6343

media@hhs.gov

U.S. Surgeon General Issues Advisory on Youth Mental Health Crisis Further Exposed by COVID-19 Pandemic

Today, U.S. Surgeon General Dr. Vivek Murthy issued a new Surgeon General's Advisory to highlight the urgent need to address the nation's youth mental health crisis. As the nation continues the work to protect the health and safety of America's youth during this pandemic with the pediatric vaccine push amid concerns of the emerging omicron variant, the U.S. Surgeon General's Advisory on Protecting Youth Mental Health outlines the pandemic's unprecedented impacts on the mental health of America's youth and families, as well as the mental health challenges that existed long before the pandemic.

The Surgeon General's advisory calls for a swift and coordinated response to this crisis as the nation continues to battle the COVID-19 pandemic. It provides recommendations that individuals, families, community organizations, technology companies, governments, and others can take to improve the mental health of children, adolescents and young adults.

"Mental health challenges in children, adolescents, and young adults are real and widespread. Even before the pandemic, an alarming number of young people struggled with feelings of helplessness, depression, and thoughts of suicide — and rates have increased over the past decade," said **Surgeon General Vivek Murthy**. "The COVID-19 pandemic further altered their experiences at home, school,

MPRnews

 SIGN IN

 NPR SHOP

 DO

 MUSIC

 PODCASTS & SHOWS

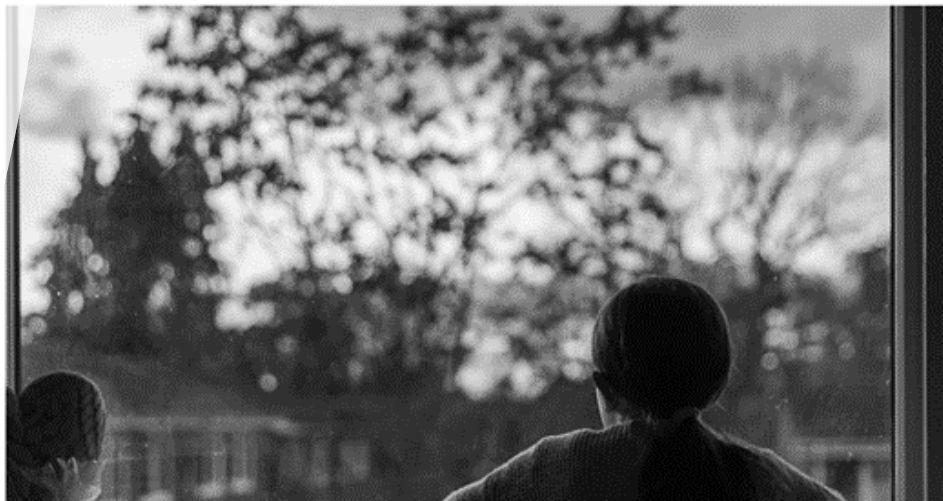
 SEARCH

CHILDREN'S HEALTH

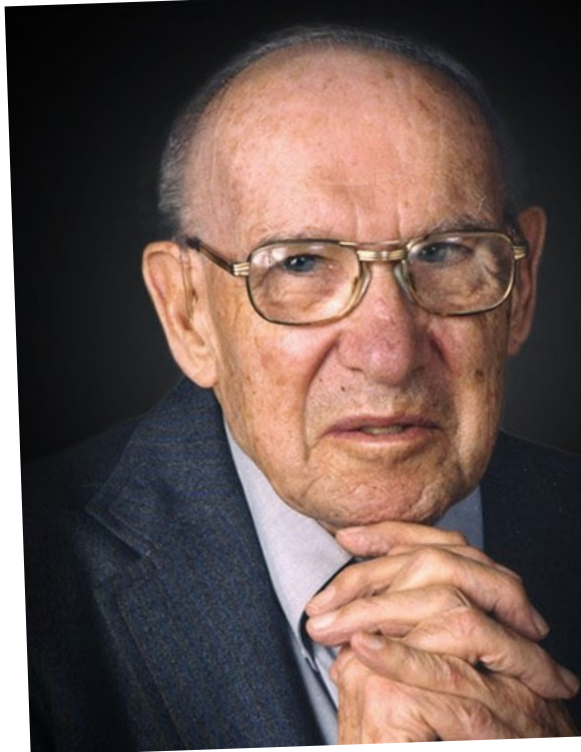
Pediatricians say the mental health crisis among kids has become a national emergency

October 20, 2021 · 3:50 PM ET

DEEPA SHIVARAM







The greatest **danger** in times
of turbulence is not the turbulence;
it is to **act with yesterday's logic.**

— *Peter Drucker*

Creating Fearless Environments

(The Critical Role of Psychological Safety)

***“No one comes up
with a good idea
when being chased by
a tiger”***



~ Anonymous board member of Tesla to
Elon Musk as quoted by *Wired* in DR. ELON &
MR. MUSK

Psychological Safety Defined

a belief that one will **not be punished or humiliated** for speaking up with ideas, questions, concerns or mistakes.



Psychological Safety is the soil, not the seed

~ Professor Amy C. Edmondson



Effective Teams

- Inclusion & Diversity
- Willingness to Help
- Attitude Toward Risk & Failure
- Open Communication



**So why are not all
teams safe?**

Impression Management

No one wants to look	It's easy to manage
Ignorant	Don't ask questions
Incompetent	Don't admit weakness or mistake
Intrusive	Don't offer ideas
Negative	Don't critique the status quo

The Dangers of Low Psychological Safety



Dangerous Silence: people who are aware of the risks of a situation, do not dare to speak up for fear of being called out or punished for it.

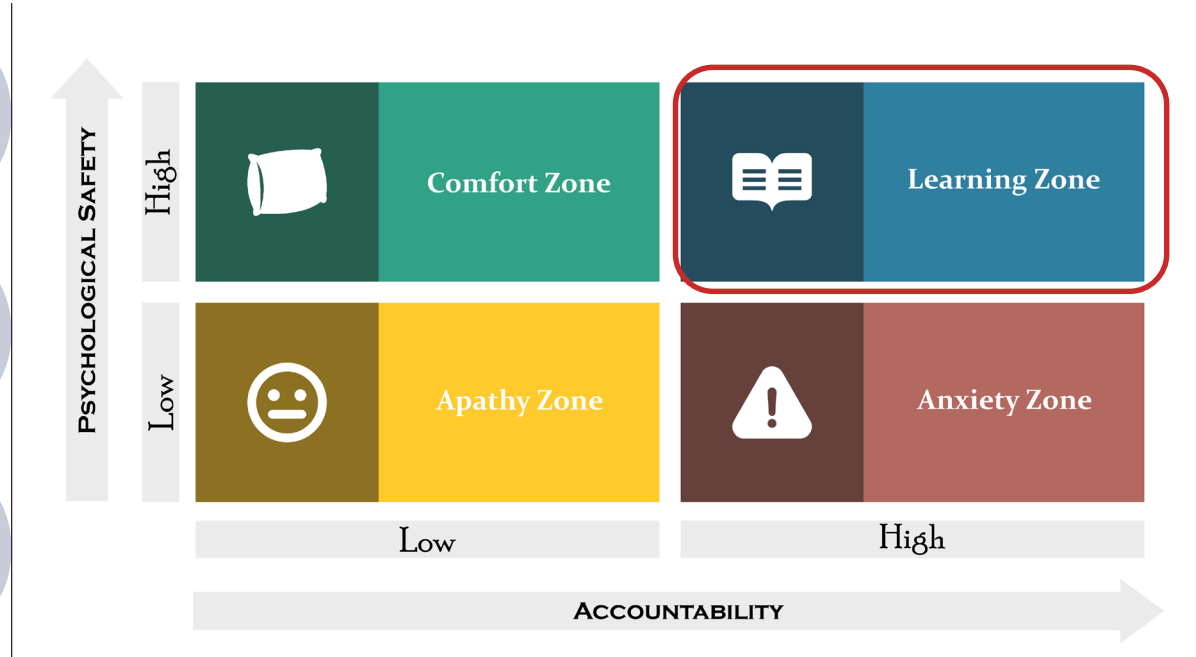


Avoidable Failure: people are more focused on avoiding failure than getting the most out of work. Also, people tend to make more mistakes that could have been avoided.

It is not
primarily
about feeling
good, it is
about **high
performance.**



Psychological Safety & Accountability



**Compared with
people at low-
trust
companies,
people at high-
trust
companies
report:**

- **74% less stress**
- 106% more energy at work
- 50% higher productivity
- 13% fewer sick days
- 76% more engagement
- 29% more satisfaction with their work
- **40% less burnout**

Thank you for bringing this forward; I'm sure it wasn't easy.

What do you need more/less of from me?

This is new territory for us, so I need everyone's input.

Things are happening and changing fast. We will make some mistakes and that's okay.

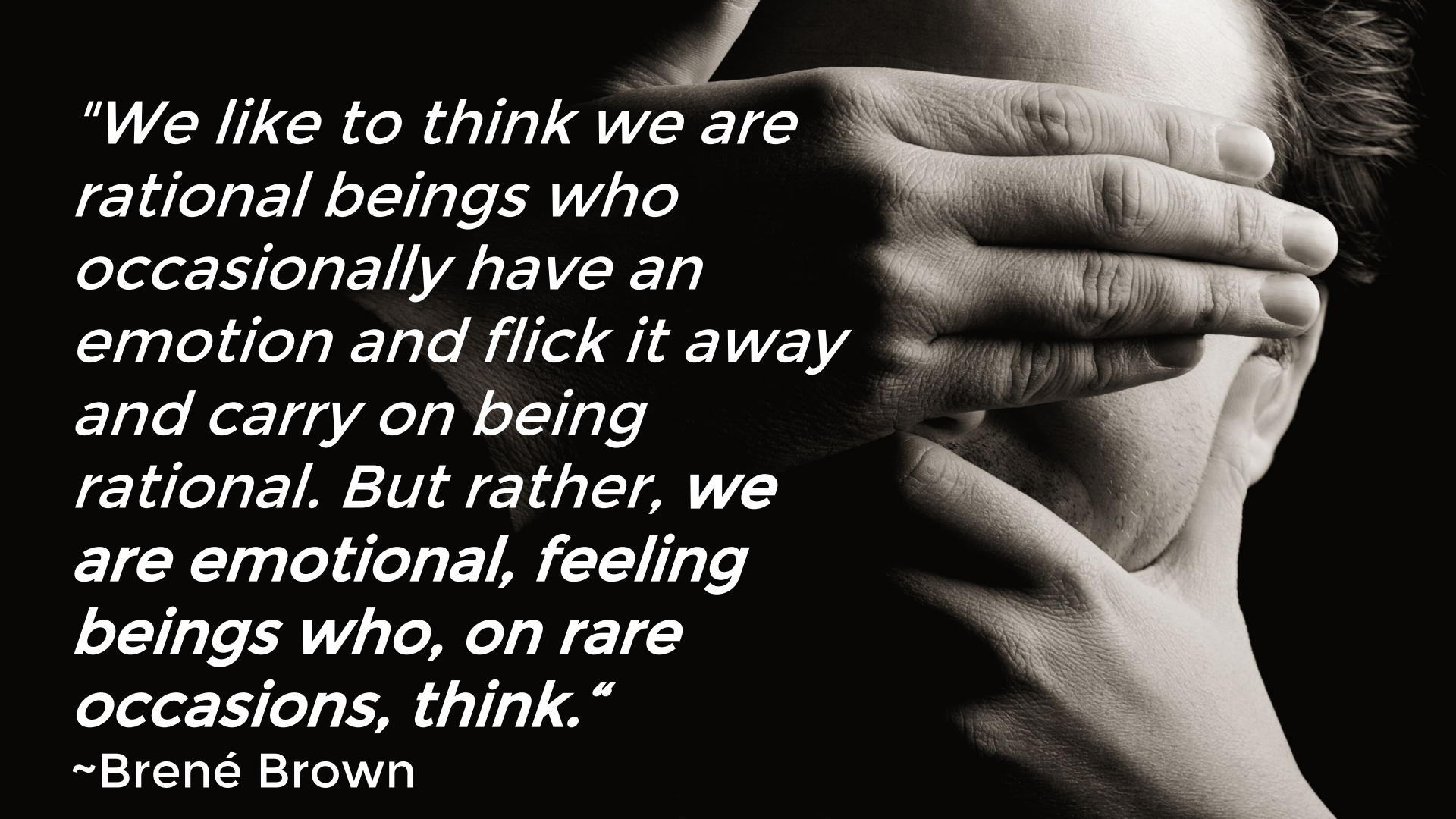
What are the biggest missteps you had this past week? What valuable lessons did they provide?

What's getting in your way? What support do you

Who has another way of looking at this? Let's hear a perspectives.

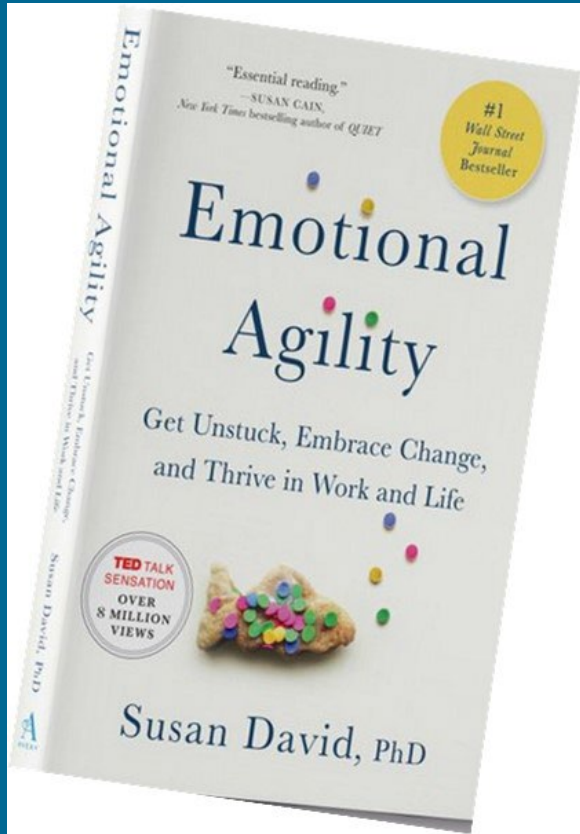
Giving Ourselves & Others Permission to Feel

(A Key Aspect of Psychological Safety)



"We like to think we are rational beings who occasionally have an emotion and flick it away and carry on being rational. But rather, we are emotional, feeling beings who, on rare occasions, think."

~Brené Brown



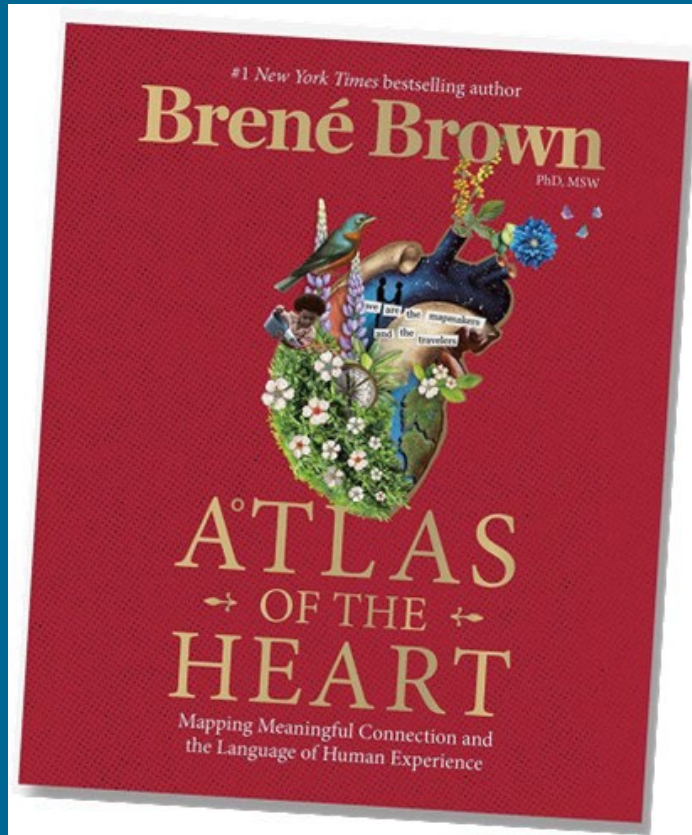
“A process that enables us to navigate life's twists and turns with self-acceptance, clear-sightedness, and an open mind.”

“

*Leaders must either invest a reasonable amount of time attending to fears and feelings, or **squander an unreasonable amount of time trying to manage ineffective and unproductive behavior.***

”

Brené Brown



*“Language is our portal to meaning-making, connection, healing, learning and self-awareness...
When we don’t have the language to talk about what we’re experiencing, our ability to make sense of what’s happening and share it with others is severely limited.”*

Why This Matters...



People will do almost anything to not feel pain



Without accurate language, we struggle to get the help we need, and we don't always regulate or manage our emotions and experiences in a way that allows us to move through them productively



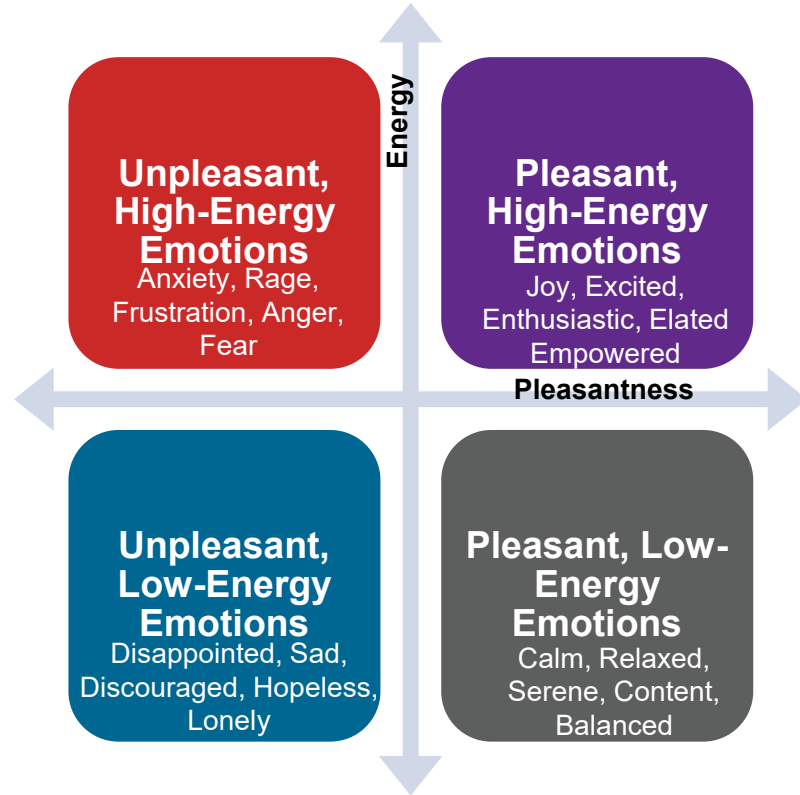
Ability to name emotion or experience is essential to being able to process it in a productive and healing manner

Emotional & Change Agility:

1. *Where am I/ are we?*
2. *How did I/we get here from there?*
3. *How do I/we get there from here?*

Become an Emotion Scientist

- **R**ecognize
- **U**nderstand
- **L**abel
- **E**xpress
- **R**egulate





HELP

Accurate Language Matters!

Stressed:

- When we evaluate environmental demand as **beyond our ability to cope successfully**

Emotional reaction more tied to our cognitive assessment of whether we can cope than how our body is reacting

Overwhelmed:

- An extreme level of stress, an emotional and/or cognitive intensity to the point of feeling **unable to function.**

**Only remedy is NOTHING-ness*

Resentment...

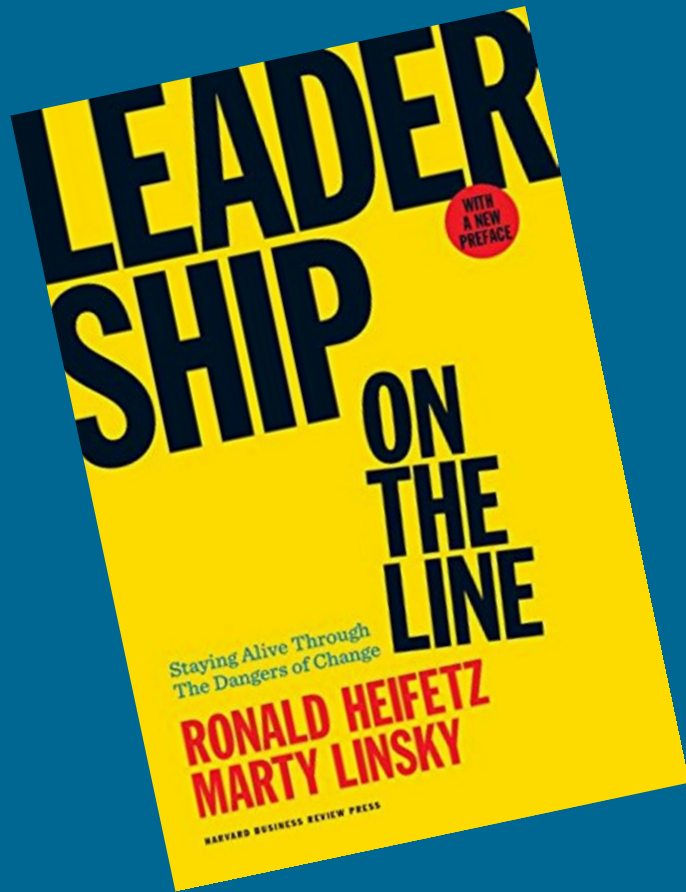
isn't a form of Anger, it's part of ENVY

Difficult Emotions





**WARNING
ANGER**



“Without learning new ways – changing attitudes, values and behaviors – people cannot make the adaptive leap necessary to thrive in the new environment.”

Being Self-Aware

*(Managing Triggers to “Armor Up” to Not
Get Hijacked By Unpleasant Emotions)*

The Frame





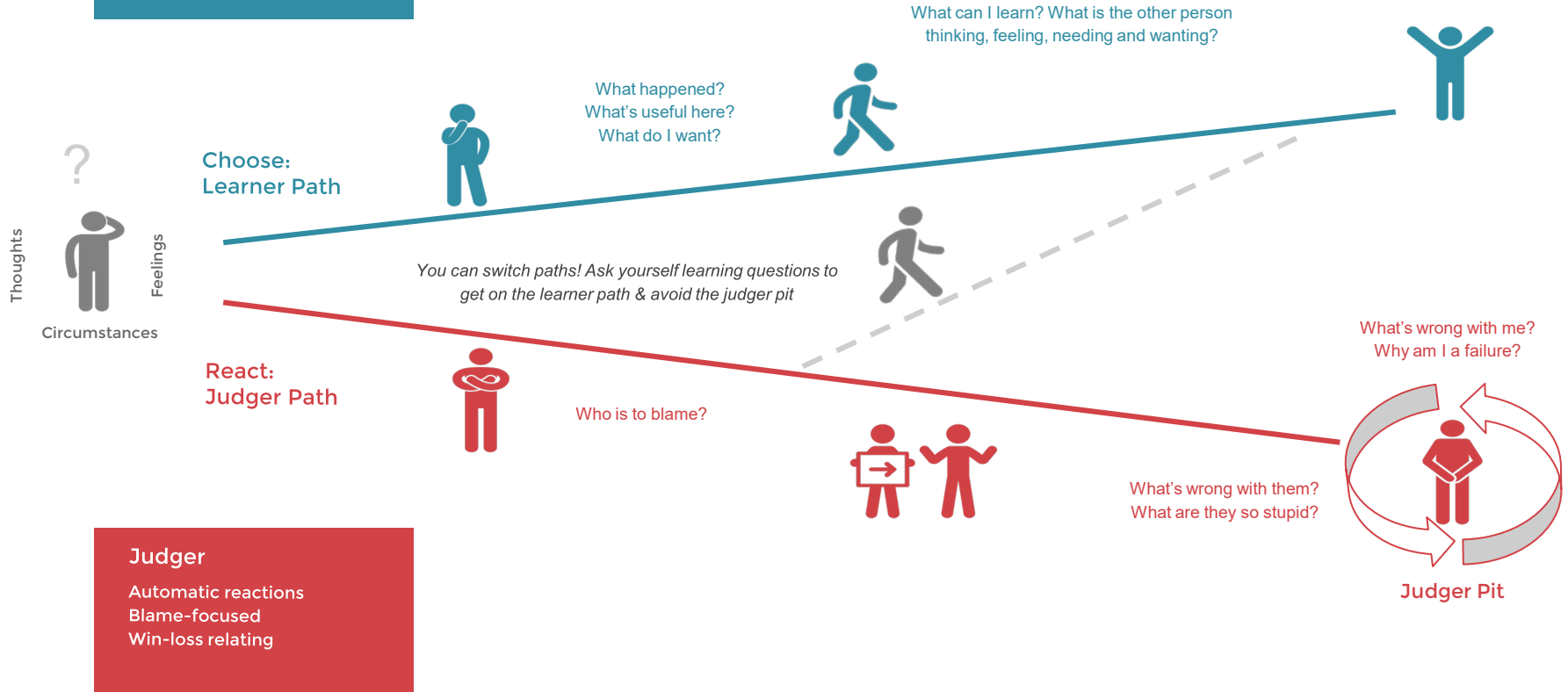
Maximize Reward / Minimize Threat

- **S**tatus
- **C**ertainty
- **A**utonomy
- **R**elatedness
- **F**airness

Learner vs. Judger

Learner

Thoughtful decisions
Solutions-focused
Win-win relating



Judger

Automatic reactions
Blame-focused
Win-loss relating

The Choice Line

Source: Jim Dethmer, Diana Chapman & Kaley Warner Klemp (*The 15 Commitments of Conscious Leadership*)

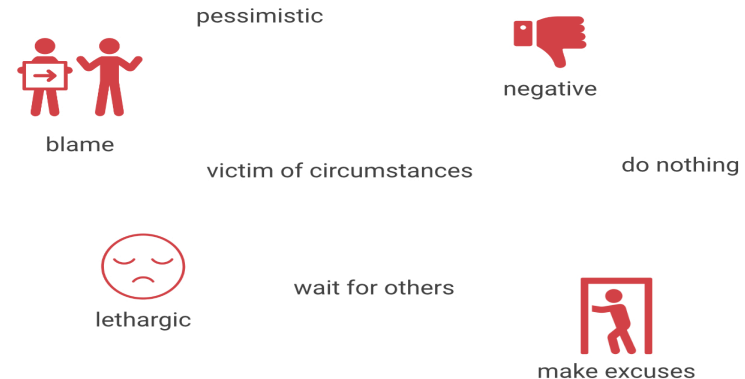


ABOVE THE LINE

proactive thinking and behaviors

BELOW THE LINE

reactive thinking and behaviors



Inward Mindset



See People as OBJECTS:

- Vehicles
- Obstacles
- Irrelevant

Inward Mindset Behaviors

Hard Behaviors			Soft Behaviors		
Vehicles	Obstacles	Irrelevant	Vehicles	Obstacles	Irrelevant
Manipulate	Criticize	Ignore	Indulge	Cope	Engage in token niceties
Threaten	Blame	Exclude	Pander	Avoid	Offer little feedback
Control	Punish	Belittle	Try to be liked	Leave	

The Self-Deception Box

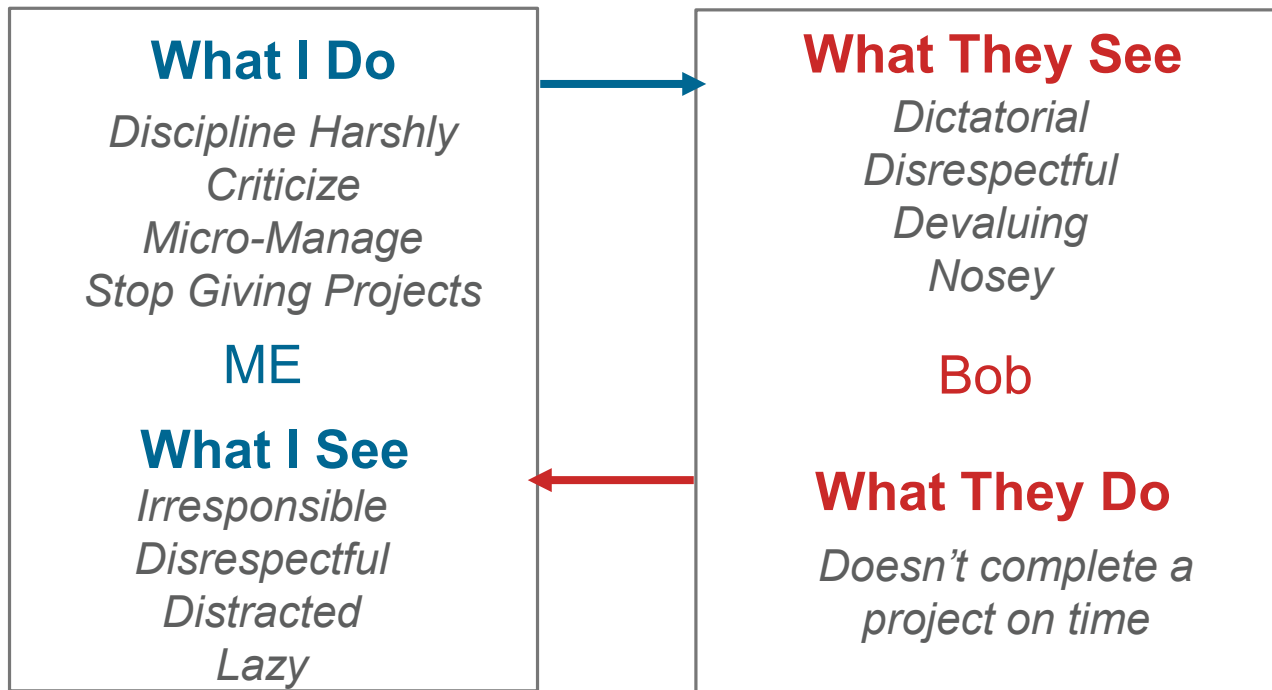
How I Start to See MYSELF:

- Victim
- Hard Working
- Important
- Fair
- Sensitive

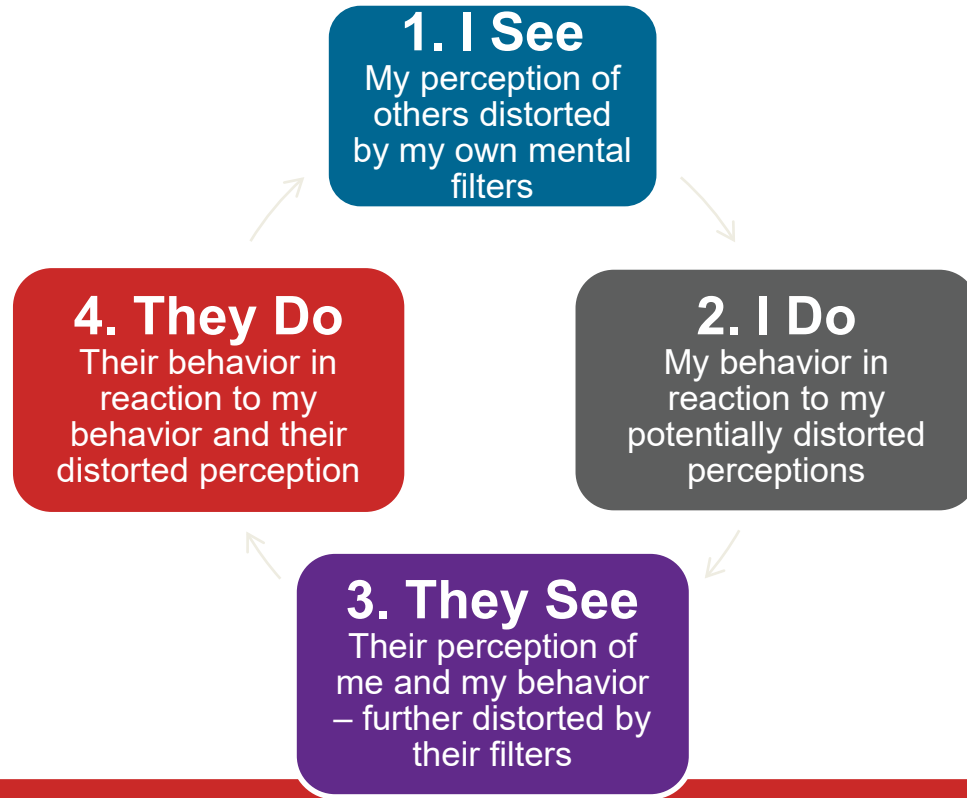
How I Start to See OTHERS:

- Lazy
- Inconsiderate
- Unappreciative
- Insensitive
- Faker

The Self-Deception Cycle



Cycle of Collusion




**P
A
U
S
E**

Move from *Ego* to *Self-Reflection*

The *Ego* is our filter on reality – leading us to:

- Please
- Perform
- Perfect
- Self-Protect



**Stop believing
everything you think!**

Showing Up Courageous

(Replacing Armor to Maximize Our Effectiveness)

Building Grounded Confidence to Replace Armor

**Grounded Confidence =
Rumble Skills + Curiosity
+ Practice**



Balcony vs. the Dancefloor



The 5 C's of Strategic Decision-Making

- Color
- Context
- Connective Tissue
- Cost
- Consequences



5 C's Reflection

Share a “just get it done” delegation experience where you were the delegator or the delegate; walk through if and how the 5Cs would have:

- Helped in producing a better deliverable
- Helped someone understand how their work contributes to a larger strategy
- Provided a teaching moment
- Offered a space for feedback on a better way to get something done

A stone archway made of rough, grey stones. A bright, warm light shines through the opening of the arch, creating a strong lens flare effect that illuminates the scene. The light is most intense in the center of the arch and fades towards the edges. The ground in front of the arch is covered in dry, brown leaves and twigs.

Replacing **Armor**

- **Rumble Starters**
- **Rumble Tools**

with Curiosity

Rumble Tools Reflection

- How could the Rumble Starters and Tools help you navigate change?
- What gets in your way of **leaning into / rumbling with vulnerability?**



**What's One
Thing You're
Taking Away
From This
Session?**

Rosie Ward, Ph.D., MPH, MCHES, BCC, CIC®

Salveo Partners LLC

Rosie@SalveoPartners.com

(877) 373-6850

www.SalveoPartners.com

www.DrRosieWard.com

Thank you for attending this event!

- Please provide your feedback using the link or QR code below:
- <https://www.surveymonkey.com/r/XNVSZDJ>

