



APPLIED RESEARCH LAB
FOR INTELLIGENCE
AND SECURITY

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

**Defining Insider TRUST
(Trustworthy, Reliable, and Useful Systems and
Teams)**

Final Report

September 30, 2021

Kelly M. Jones*¹, Bernadette Jerome¹, Jordan C. Roberts¹, Emily Pitek¹, Graduate Student 1¹⁺,
& Adam Russell¹

¹Applied Research Laboratory for Intelligence and security

+name withheld at author's request

*Corresponding author, kjones@arlis.umd.edu

EXECUTIVE SUMMARY

Task 1 under the ARLIS FY20 Countering Insider Threat program of research focused on scoping and defining ARLIS's Insider TRUST (Trustworthy, Resilient, and Useful Systems and Teams) approach. Insider TRUST research is designed to complement the traditional approach of addressing insider threats (the detect, deter, and mitigate approach) by providing a framework of concepts and research that could be practically applied to cultivate healthy work environments that reduce the risk of insider events and/or empower individual, organizational, and mission success.

The goal of this task has been to provide a starting point for addressing complex sociotechnical problems of the *human domain* by *integrating* existing research across multiple disciplines (with particular emphasis on drawing from social and behavioral science disciplines not often incorporated into security research) to create a broad base of concepts and knowledge that are potentially applicable to countering and mitigating risks of insider events, and *creating* new research by drawing on ARLIS ability as a UARC to *convene* experts across silos of information to identify the best ways forward in developing future operationally focused research questions related to the larger program of research on insider risk/threat at ARLIS.

We conducted a literature review of concepts related to Insider TRUST (e.g., resilience, burnout, organizational behaviors), and built conceptual models of the relationships between constructs based on the literature. The team developed a list of questions we then posed to subject matter experts (SMEs) in a semi-structured interview, regarding the constructs identified as potentially relevant to understanding and modeling Insider TRUST, additional constructs to be included, as well as potential relationships between these constructs. The goals of the research were to 1) identify common themes and questions among insider threat operators, researchers, and policymakers, 2) develop, refine, and expand the conceptual model of relevant constructs, and 3) develop future operationally focused research questions related to the larger program of research on insider risk/threat at ARLIS.

We noted four major recurring themes across the majority of our work.

1. *The importance of trust.* The need for solid foundational research on the relevance of trust to reducing insider risk, how to best assess trust, how best to increase trust, and the importance of trust as a part of leadership and workplace relationships were all raised as key questions for future research.
2. *The importance of good leadership and good relationships with colleagues.* The importance of cultivating and maintaining strong, healthy, and supportive relationships between colleagues, between immediate supervisors and supervisees, and between organizational leadership and employees was repeatedly highlighted. However, the greatest emphasis was given to the importance of good leadership at every level throughout an entire organization. Key future applied research questions focused on effectiveness and content training to organizational leaders to build TRUST through best leadership practices (e.g., demonstrating respect and valuing employees, setting and living up to organizational standards and expectations, clear communication).

3. *De-emphasis on tracking individual characteristics, and the need for greater emphasis on organizational characteristics.* Individual factors (e.g., personality, individual motivation, burnout) which currently receive great attention, were largely de-emphasized in favor of greater focus on organizational level factors such as leadership and the perceptions of organizational policies (including insider threat programs). When individual characteristics were mentioned by SMEs, they focused more on positive characteristics that can be fostered (e.g., resilience, well-being), rather than on the innate characteristics which can sometimes be negative (e.g., personality, pessimism).
4. *Recognition of the difficulty in, but ultimate importance of, getting ahead of threats before they manifest.* The security challenges, and opportunities, of insider risk/threat and personnel vetting are problems of the human domain, requiring successfully integrating the social and behavioral sciences in concert with technical solutions to better measure and model (characterize, quantify, predict) and mitigate (shape, exploit, prevent) emergent insider risks/threats. Gaining and maintaining advantage in human domains requires proactive, rather than reactive, interventions. By recognizing and operationalizing new predictors and indicators of increased risk, the security community will be able to build a resilient and trusted workforce – one that is much less likely to produce detrimental surprise. For example, rather than just assuming that a focus on threats informed largely by case studies of “what went wrong” in organizations is the best approach to Insider Threat, might we stand to gain from also trying to understand “what goes right” in high performing organizations where things like building and maintaining trust among an organization and its personnel are also prioritized?

A sample of possible applied research questions proposed either by the team or SMEs:

1. How do we take into account trustworthiness variables in our calculations of risk? How do we build systems that consider trustworthiness (and training, resilience, and other social behavioral factors) in risk assessments?
2. How do insider threat programs, leaders, and organizations, best build and communicate shared visions of addressing insider risk and building Insider TRUST? How effective are such messages in decreasing risk? Who are the best messengers of shared visions – leaders?
3. Is an effective way to build Insider TRUST through identifying and training leaders (and future leaders) in best leadership practices (e.g., demonstrating respect and valuing employees, setting and living up to organizational standards and expectations, clear communication)?
4. What elements of best leadership practices will remain constant over time and what will need to change in order to retain our advantage in the human domain?
5. What theoretical models for decision making can be leveraged or built for insider risk and Insider TRUST? How can we effectively draw research from other fields (e.g., game theory, Industrial/Organizational psychology, management, communications, risk-based decision making), making sure that what we draw is relevant and applicable for insider risk/threat contexts (both the theoretical model and its foundational concepts)?
6. What is the effect of the information environment on insider risk/threats and Insider TRUST? Do belief polarization and disinformation contribute to increased risk of insider

events? If they do, what are the best techniques for decreasing risks of insider events that are influenced by disinformation?

7. What is the larger organizational ecosystem from which insider risks emerge? What is the best way to model that ecosystem?
8. How do we link research, and operational best practices, that addresses the immutably sociotechnical nature of the human domain challenges we face across the entire interdependent supply chain of products, services, workforces, and workplaces?

The fourth key theme our SMEs identified is that gaining and maintaining advantage in human domains requires proactive, rather than reactive, interventions. The above applied research questions represent one approach to proactive work - identifying key questions in a research portfolio on addressing insider risk/threat and creating Insider TRUST.

Contents

EXECUTIVE SUMMARY 2

Defining Insider TRUST 6

(Trustworthy, Resilient, and Useful Systems and Teams)..... 6

 What is the problem we are trying to solve? And what difference would it make when we do?..... 7

BLUF (Bottom Line Up Front) – Recurring themes of note..... 7

Method 9

Literature Review..... 9

 Most Important Constructs for Insider TRUST 10

 Trust and Trustworthiness 10

 Leadership 13

 Sub-Constructs Linking Leadership and Trust/Trustworthiness 16

 Group and Team Dynamics..... 21

 Organizational Citizenship Behaviors and Counterproductive Workplace Behaviors..... 22

 Wellbeing and Resilience..... 23

 Least Important Factors to Insider TRUST 25

 Personality..... 25

 Individual Difference Factors & Optimism..... 26

Subject Matter Expert Interviews..... 27

 Methods 27

 Participants 27

 Procedure and Interview Protocol..... 28

 Data Analysis 28

 Results 29

Conclusion 42

ACKNOWLEDGEMENTS..... 42

DISCLAIMERS..... 44

ABOUT ARLIS 44

 Technical Points of Contact: 44

 Administrative Points of Contact:..... 44

REFERENCES..... 45

Appendix 1: Applied Research Questions 52

APPENDIX 2: Construct Maps..... 59

APPENDIX 3: Subject Matter Expert Interview Materials 67

 Semi-structured interview protocol 67

 Question 3 Materials for Construct Sort..... 68

Construct Definitions	69
-----------------------------	----

Defining Insider TRUST (Trustworthy, Resilient, and Useful Systems and Teams)

In FY20, ARLIS proposed a complimentary method to the traditional “Detect, Deter, and Mitigate” approach to countering insider risk/threats. We named this approach Insider TRUST for Trustworthy, Resilient, and Useful Systems and Teams. Insider TRUST research is designed provide a framework that can be practically applied to cultivate healthy work environments that reduce the risk of insider events and/or empower individual, organizational, and mission success.

Over FY20, ARLIS has completed its first work in scoping and defining the Insider TRUST approach, drawing from both existing empirical research and conducting interviews with subject matter experts in relevant fields. We began this work with the acknowledgement that no single research project could encompass all possible ideas or research relating to countering insider risk/threats¹, or empowering individual, organizational, and mission success. The goal of this research has been to provide a starting point by *integrating* existing research across multiple disciplines (with particular emphasis on drawing from social and behavioral science disciplines not often incorporated into security research) to create a broad base of concepts and knowledge that are potentially applicable to countering and mitigating risks of insider events, and *creating* new research by drawing on ARLIS ability as a UARC to *convene* experts across silos of information to identify the best ways forward in developing future operationally focused research questions related to the larger program of research on insider risk/threat at ARLIS.

¹ *A note on terminology: As reflected throughout our work across the entire program of research, the ARLIS team prefers the term “insider risk” rather than “insider threat.” The study and management of risk plays an integral role in physical, personnel, information, and other forms of security and the application of Insider Threat paradigms. Yet, much of source and contextual details, modeling options, and solution space nuances are lost when insider as a risk is reduced to insider as a threat. Shifting to Insider Risk requires substantial reframing from management based on threat elimination toward dynamic situational management where risk is a variable dependent on situational tolerance and requires ongoing consideration for the interaction of individual and contextual variables. This effort emphasizes active decision-making and aids in the measurement of consequence and risk. People remain a central focus but shift to be part of the solution in helping reduce risk of any kind. However, for clarity we will refer to insider risk/threat throughout this report, since threat is still the most widely used terminology.

What is the problem we are trying to solve? And what difference would it make when we do?

Although “insider threat” was not a new term (or concept), several high-profile incidents in the early 2000s prompted Executive Order 13587, establishing a set of structural reforms at the federal level to improve the protection of classified information including the formation of the National Insider Threat Task Force in October of 2011. The following November, the Minimum Standards for federal insider threat programs were released, followed by the Maturity Framework in 2018. Simultaneously, the scope and focus of Counter Insider Threat programs has grown beyond their initial focus (at the federal government level) on espionage and unauthorized disclosure of classified information, to encompass a diverse set of adverse events including fraud, sabotage, loss of sensitive but unclassified information, workplace violence, and suicide.

While the majority of research and work in countering insider risk/threat has understandably focused on the prevention of harm, there is an inherent limitation in the ability of such work to mitigate risk in that it almost always focused solely on the deterrence of negative behaviors, either through the prevention/denial of opportunities to engage in the behavior (e.g., controlling access to systems), or the identification and reporting of negative behaviors by colleagues and supervisors. Further, traditional security focused approaches using the detect, deter, mitigate model tend to rely heavily on technical-focused interventions, such as cybersecurity measures, user activity monitoring software, and continuous evaluation of personnel via automated data collection (such as credit reports or arrest records).

Both the NITTF Maturity Framework (2018) and the FY2020 -2024 DoD Counter-Insider Threat Program Strategic Plan, identifies social and behavioral science, one of ARLIS’s core competencies, as crucial to understanding of and gaining advantage in the human domains of vetting personnel and mitigating insider risk/threat. The human domain is any domain where understanding human sociotechnical diversity, networks, systems, beliefs, strengths, limitations, and vulnerabilities confers advantage. Insider risk/threat is a complex problem which requires balancing technical and human centered approaches to address. Insider TRUST brings social and behavioral science concepts to the human domain problem of addressing insider risk/threat. It widens the scope of focus beyond the individual to include organizational and group level factors. And, in theory, identifying and addressing such factors can mitigate risks prior to them becoming threats.

BLUF (Bottom Line Up Front) – Recurring themes of note

Though each SME (both internal to the team and our interviews with external SMEs) emphasized different constructs, and posed different suggestions/future questions, we noted four major recurring themes across the majority of our work – both through our review of the literature and our interviews with SMEs.

1. *The importance of trust.* Perhaps one of the broadest concepts we investigated, trust has multiple definitions across different settings, but generally refers to a situation in which one

party must rely in some way on the actions of another (e.g., Mayer, Davis, & Schoorman, 1995; Williams, 2001). Every SME presented with this construct ranked it “most important,” and it was the second most frequent spontaneously generated concept discussed for inclusion in Insider TRUST by our SMEs. Both the positive aspects of trusting and being trusted were raised as possible avenues to explore in future work on reducing insider risk, as well as the negative aspects that can occur in the absence of trusting and being trusted. Further, the need for solid foundational research on the relevance of trust to reducing insider risk, how to best assess trust, how best to increase trust, and the importance of trust as a part of leadership and workplace relationships were all raised as key questions for future research.

2. *The importance of good leadership and good relationships with colleagues.* Originally, we considered these as separate constructs, but conversations with SMEs revealed significant overlap across constructs focusing on relationships in the workplace. SMEs heavily emphasized the importance of cultivating and maintaining strong, healthy, and supportive relationships between colleagues, between immediate supervisors and supervisees, and between organizational leadership and employees. However, the greatest emphasis was given to the importance of good leadership at every level throughout an entire organization. The majority of the specific recommendations from SMEs for immediate operationalization of Insider TRUST focused on providing training to organizational leaders, both to directly address insider risk/threat (e.g., recognizing concerning behaviors, reporting requirements) and to build TRUST through best leadership practices (e.g., demonstrating respect and valuing employees, setting and living up to organizational standards and expectations, clear communication).
3. *De-emphasis on tracking individual characteristics, and the need for greater emphasis on organizational characteristics.* Though not specifically mentioned by any single SME, when viewing the summation of their recommendations, it became clear that individual factors (e.g., personality, individual motivation, burnout) which currently receive great attention, were largely de-emphasized in favor of greater focus on organizational level factors such as leadership and the perceptions of organizational policies (including insider threat programs). When individual characteristics were mentioned by SMEs, they focused more on positive characteristics that can be fostered (e.g., resilience, well-being), rather than on the characteristics that are innate to individuals which can sometimes be negative (e.g., personality, pessimism).
4. *Recognition of the difficulty in, but ultimate importance of, getting ahead of threats before they manifest.* The security challenges, and opportunities, of insider risk/threat and personnel vetting are problems of the human domain, requiring successfully integrating the social and behavioral sciences in concert with technical solutions to better measure and model (characterize, quantify, predict) and mitigate (shape, exploit, prevent) emergent insider risks/threats. Gaining and maintaining advantage in human domains requires proactive, rather than reactive, interventions. By recognizing and operationalizing new predictors and indicators of increased risk, the security community will be able to build a resilient and trusted workforce – one that is much less likely to

produce detrimental surprise. For example, rather than just assuming that a focus on threats informed largely by case studies of “what went wrong” in organizations is the best approach to Insider Threat, might we stand to gain from also trying to understand “what goes right” in high performing organizations where things like building and maintaining trust among an organization and its personnel are also prioritized?

Method

As noted earlier, no single research project could encompass all possible ideas or research relating to countering insider risk/threats, or empowering individual, organizational, and mission success. What follows is in no way a complete list of all the relevant constructs or research but is instead a sample of constructs across multiple academic disciplines including psychology, sociology, business, management, and others. We conducted a literature review of concepts related to Insider TRUST (e.g., resilience, burnout, organizational behaviors), and built conceptual models of the relationships between constructs based on the literature. The initial list of concepts was compiled from research conducted during the FY19 program, as part of the team’s work to develop the first conceptualization of Insider TRUST. Further constructs were added during the literature review conducted under this program, and from discussions with internal and external subject matter experts (SMEs).

From this literature review, the team developed a list of questions we then posed to subject matter experts in a semi-structured interview, regarding the constructs identified as potentially relevant to understanding and modeling Insider TRUST, additional constructs to be included, as well as potential relationships between these constructs. The semi-structured interview format allowed for back-and-forth conversation regarding the interviewee’s expertise and opinions regarding important questions that should be addressed in future research. The goal of the literature review in combination with the SME interviews was to 1) identify common themes and questions among insider threat operators, researchers, and policymakers, 2) develop, refine, and expand the conceptual model of relevant constructs, and 3) develop future operationally focused research questions related to the larger program of research on insider risk/threat at ARLIS.

Literature Review

As will be reviewed in greater detail in the later section regarding our interviews with SMEs, their responses during interviews were meant to help narrow the focus of our wide-ranging literature review efforts by identifying common themes and most important topics. This section is consequently ordered based on SME characterization of the constructs most important to least important in addressing insider risks and building Insider TRUST.

Most Important Constructs for Insider TRUST

Trust and Trustworthiness

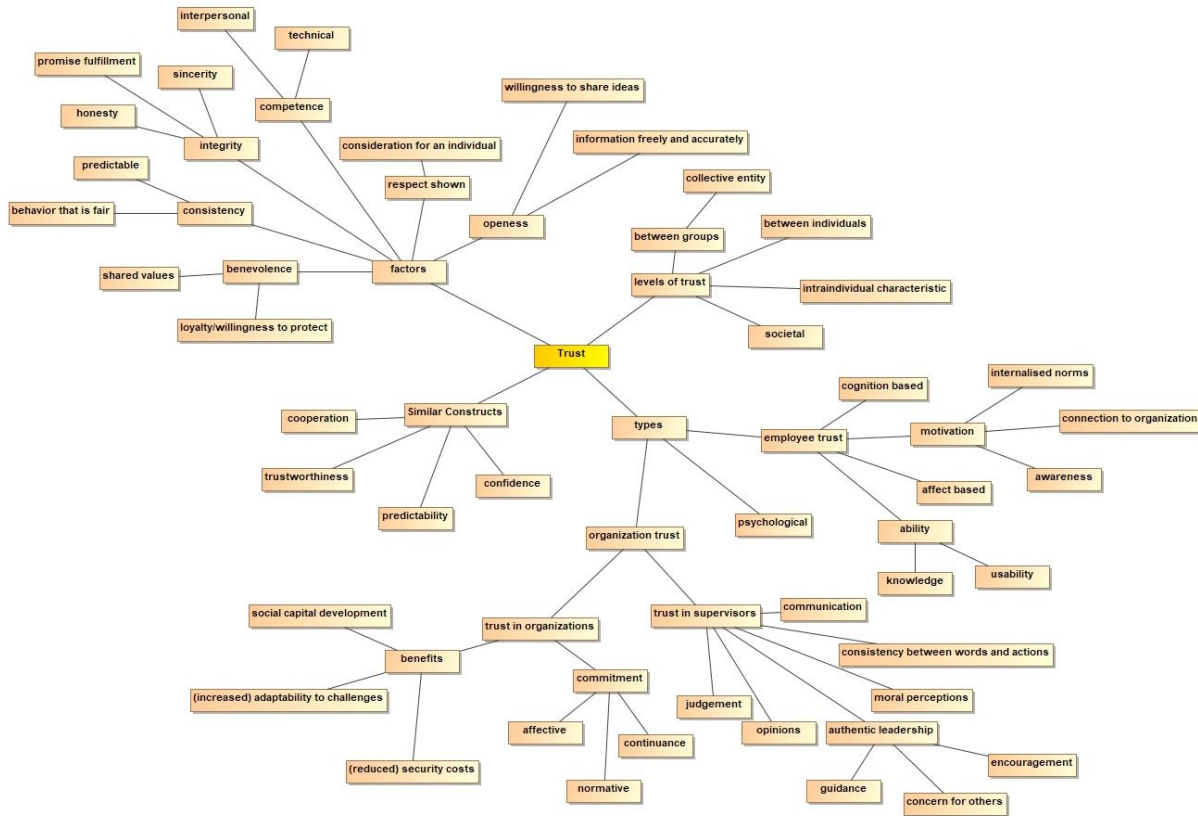
“If people feel trusted, most people will want to live up to that trust”
-SME #5

Trust has been recognized across multiple disciplines as a crucial component to the success of organizations. On the individual level, it is linked to positive outcomes including teamwork (Sargent & Waters, 2004), effective leadership (Dirks & Ferrin, 2002), and employee

satisfaction, effort, and performance (Colquitt, Scott, & LePine, 2007; Edwards & Cable, 2009). At the organizational level, higher levels of trust allow organizations to focus on long term goals and effective organizational change (Koçyiğit & Akkaya, 2020) and employee engagement (Wang & Hseih, 2013).

Decades of trust research, across multiple disciplines, has produced dozens of definitions of trust. The broadest and most consistently cited definition comes from Mayer, Davis, and Schoorman (1995), “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party,” (pp. 712). This definition encompasses trust at multiple levels within groups, and across different relationships. For example, within a single organization, a person may (or may not) have trust in another individual (e.g., Lewicki, Tomlinson, & Gillespie, 2006), with their team (e.g., Feitosa, Grossman, Karamer, & Salas, 2020), or with their organization. Likewise, an organization, a team, or another individual may (or may not) have trust in the first individual. Further, trust and trustworthiness are linked to a wide range of other constructs and factors in the literature (see Figure 1 below for construct map created by the team).

Figure 1: Trust Construct Map - Relationships to Other Constructs Identified in the Literature



Given the emphasis of our work, we focused on research regarding trust in organizations and the workforce. Much of the research on workplace trust focuses on the interpersonal level (trust between two individuals, such as an employee and their supervisor). There are largely two paradigms of research here – one paradigm differentiates between dimensions of trust as cognitive, based on rational calculation, or affective, based on emotional attachment; the second paradigm differentiates between factors that indicate trustworthiness of an individual (ability, benevolence, behavioral integrity, and values congruence), and interpersonal trust itself. Recent work has begun to integrate these two paradigms into a combined model which proposes several interesting, applied questions (Tomlinson, Schnackenberg, Dawley, & Ash, 2018):

1. Applied research question: what is the effect of increasing different trustworthiness indicators among leaders for creating successful workplace environments?

While most of the literature focuses on trust at the interpersonal level, there is a growing awareness of the reality that the complexity of workplace relationships means that trust must be considered at multiple levels simultaneously within sociotechnical environments. Recent work from several teams including Fulmer and Gelfand (2012), Fulmer and Dirks (2018), and Costa, Fulmer, and Anderson (2017) have proposed a multilevel-multireferent framework for trust that accounts for both trust at different levels (between individuals, teams, organizations) and trust in

different referents or targets of trust (sometimes called the trustee, this can be an individual, trust across a team, or trust in an organization as an entity). Multilevel models of trust allow for applied research questions that include cross levels effects, such as testing the impacts of changes in trust in one's supervisor to changes in trust towards one's organization or vice versa. Further, it opens the door to more complex questions including:

1. What are the effects of asymmetrical trust, where one party has a higher level of trust than the other?
2. What are the effects of shifting organizational and team boundaries, such as working with or across multiple teams or projects?
3. What are the effects of time or sudden environmental changes to trust across levels of relationships?
4. The migration of many to virtual or hybrid work environments also presents unique questions regarding the development and maintenance of trust across individual, team, and organizational levels when the traditional face-to-face interactions that form the basis of most relationships take place over electronic mediums (Hacker, Saunders, & Thayer, 2019).

Additional future research questions identified by SMEs related to trust and trustworthiness included:

1. How do we [organizations, leadership, or insider threat programs] demonstrate to employees that they are valued and trusted by their organization? How do we provide them with avenues to receive assistance when needed and/or to build resilience, skills, and capabilities?
2. How do we take into account trustworthiness variables in our calculations of risk? How do we build systems that consider trustworthiness (and training, resilience, and other social behavioral factors) in risk assessments?
3. How do insider threat programs [and leaders/organizations] consistently demonstrate to employees that they [the programs/leaders/organizations] are worthy of trust? Specifically, how can programs [leaders/organizations] demonstrate the four components of trustworthiness: ability, benevolence, behavioral integrity, and values congruence? What impact does demonstrating trustworthiness have on decreasing risk and increasing desired behaviors (such as compliance with security policies, reporting concerns)? What aspects of trustworthiness in leaders are most important to decreasing insider risk?
 - a. This was repeatedly mentioned by several SMEs, who all stressed that trust is a two-way street and must be earned on both sides – leaders and employees – though most of their focus was on leadership's actions and need to demonstrate trustworthiness and to be deserving of trust from their subordinates (see Leadership section below).
4. How do we best identify trustworthy leaders, then train them to best demonstrate trust in their supervisees? For example, training in demonstrating empathy was mentioned by several SMEs.
5. What is the perspective of those whom we ask to trust in insider threat programs, leadership, and the organization (the 'average joe' employee)?

- a. An SME rightly pointed out that much of the research on insider threat, including the current effort, focuses more on eliciting input from those already in managerial or policy positions, who likely have greater insight into the functions of insider threat programs and organizations as a whole, and that research could benefit from greater insights from those who are outside those groups.

Leadership

Similar to trust and trustworthiness, leadership has dozens of definitions across different disciplines. Generally accepted is this definition from Chemers (1991, 2000), “leadership is a process of social influence in which one person is able to enlist the aid and support of others in the accomplishment of a common task...leadership is a group activity, is based on social influence, and revolves around a common task,” (pp. 1). Chemers acknowledges that this definition makes leadership appear to be a simple task, but the reality is far more complex. Different theories emphasize different aspects of leadership and often reflect the priorities of the time in which the theory was proposed. Briefly, some key leadership theories (as summarized in Kilburg & Donohue, 2011) include:

1. Trait theories: focus is on relatively fixed or innate physical or psychological characteristics that are common or preferred in leaders (such as height or personality traits) and the relative effectiveness of these fixed characteristics within the situation or context in which the leader acts (e.g., Fleishman et al., 1991)
2. Contingency theories: focus is on leadership as a process of influencing a group towards a collaborative goal, good leaders recognize and adapt to different circumstances to remain effective, and good leaders can be trained (not born, e.g., Fiedler, 1961, 1971)
3. Style or behavioral theories*: focus is on leaders’ behavior and methods of influence, particularly leaders’ awareness of themselves and their own moral perspective, awareness of their colleagues, and ability to inspire others (e.g., Avolio & Gardner, 2007)
 - a. *We note that at least one prominent theory (authentic leadership) under this grouping has been called into question and several studies have been retracted but include here as the theory remains in use.
4. Skill or competency theories: focus is on problem solving skills and other competencies that enable leaders to successfully address ‘novel, complex, and amorphous problems’ (pp. 9), emphasis is on the ability to acquire such skills through both training and experience (e.g., Mumford et al., 2002)
5. Ecological Systems theories: leadership emerges from the interactions of all members in a system, and different levels or contexts within the system may call for different types of leadership. This grouping of theories is unique in that it places a high degree of emphasis on the role of the followers in leadership – who by their choices grant leaders legitimacy (or not), and by extension, determine a leader’s effectiveness (e.g., Yukl & Mahsud, 2010)

“The most important thing a leader can do is explain their intent, goals, and expectations. Leaders should communicate objectives, methods to complete objectives, and individual expectations, so as to empower employees to achieve organizational goals. And the most important element in a leader-follower dynamic is trust between leaders and subordinates.”

SME #6

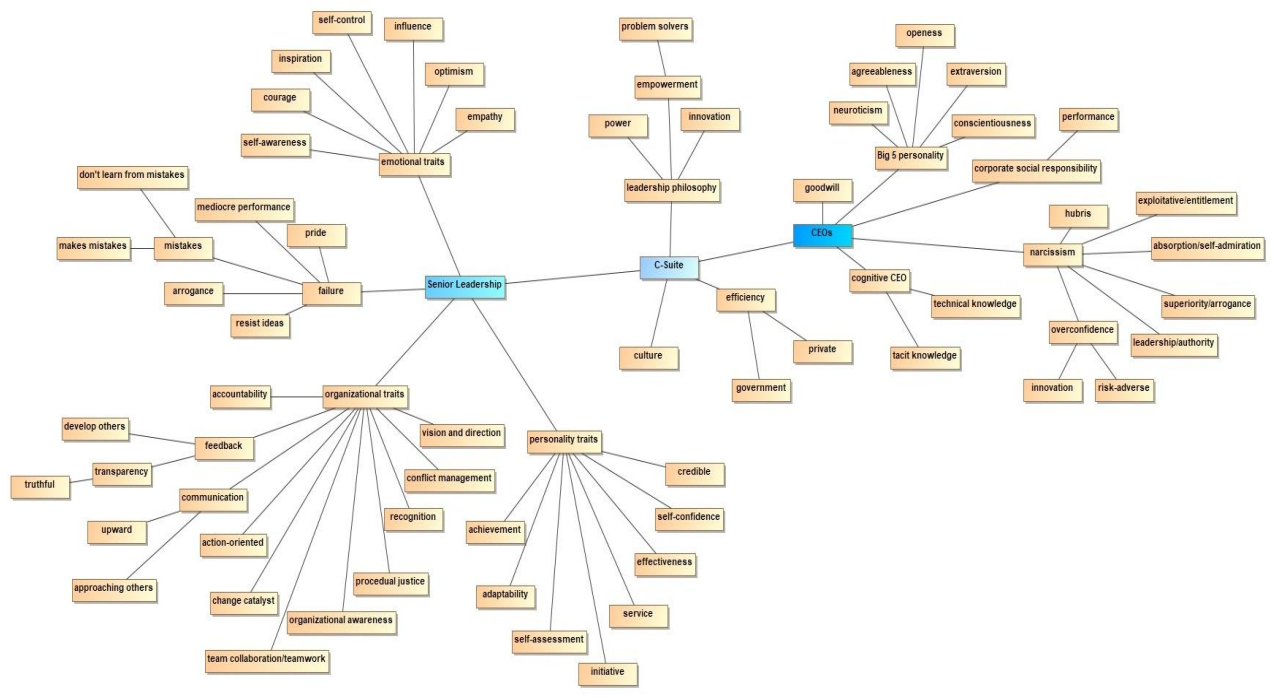
6. Leader-Member Exchange theories (including transactional versus transformational leadership styles): leadership arises from reciprocal relationships and interactions between leaders and followers, with leadership an emergent property of most groups. The most well-known is the difference between transactional leadership, which focused more supervision, organization, and evaluation of followers around performance of a task, and transformational leadership, which is focused on leadership through vision, motivation, and inspiration (e.g., Bass, 1997; Popper, Mayseless, & Castlenovo, 2000)
7. Effectiveness theories: defines leadership by its measurable outcomes or impacts on team or organizational success (e.g., Tosi, Misangyi, Fanelli, Waldman, & Yammarino, 2004)
8. Ethical or moral theories: defines leadership around leader's capabilities to address moral issues, develop character strengths in themselves and others, and set and enforce ethical standards in their organization (e.g., Sama & Shoaf, 2008)

What is consistent across this large body of research (per Kilburg & Donohue, 2011) is the acknowledgement that:

1. Leadership is emergent from complex, adaptive systems and is therefore difficult to define and measure
2. Leadership occurs at all levels of organizations, and can come from any member of that organization, not only those who are identified by title or role as leaders
3. Effective leadership comes from the successful interaction of internal factors (to the leader, to the followers, and to the organization) and external factors (culture, world events), and attempting to define or measure leadership or leadership effectiveness without contextualizing it leads to failures of over-generalization
4. Leadership is dependent on multidimensional and multidirectional relationships within and outside organizations – and all members of such relationships are important to understanding them
5. Traditional perceptions of what makes a successful leader (so-called charismatic leaders) do not necessarily equate to effectiveness of such leaders, though there are limited studies of the long-term effectiveness of different leadership styles from which to draw conclusions
6. Individual leader's self-awareness, development of leadership skills, and levels of moral reasoning can have strong effects on team and organizational success

For additional relationships identified in the literature around leadership, see Figure 2 below for construct map created by the team.

Figure 2: Leadership Construct Map – relationships to other constructs identified in the literature



In conversations with SMEs, no specific theory of leadership was particularly emphasized, but leadership was highly ranked among their ‘most important’ aspects of Insider TRUST. The majority of their suggested ways to build Insider TRUST focused on training in leadership skills, including communication, empathy, and developing and demonstrating organizational culture, and that such training should begin early and continue throughout a leader’s career.

1. Applied research question (SME suggested): How do we best identify good (potential) leaders? What training should they be provided?
 - a. SMEs repeatedly stressed the importance of training for leaders, including both training in insider risk mitigation (identification of concerning behaviors, intervention techniques, reporting requirements), but also in best leadership practices including empathy/concern, integrity, fairness, and competence.
 - b. Empirical literature supports the idea that early and continuous training for leaders is linked to increased organizational success (Longenecker & Insch, 2018), what is currently unknown is the effectiveness in decreasing insider risks/threats or increasing Insider TRUST.

Leaders who can both create and consistently communicate shared organizational vision positively influence organizational performance (Flauto, 1999; Kirkpatrick & Locke, 1996). Further, employees are active recipients of leaders’ messages who choose to connect with leaders’ visions that most closely match their own (Larson & Pepper, 2003; Postmes, Tanis, & de Wit, 2001). Employees who feel they are ‘looped in’ to building a shared vision that they believe in, and equally important feel that their leadership listens to their input on, are the most productive and creative (Argenti, 2017).

1. Applied research question: how do insider threat programs, leaders, and organizations, best build and communicate shared visions of addressing insider risk and building Insider TRUST? How effective are such messages in decreasing risk? Who are the best messengers of shared visions – leaders?

Effective leadership has also been linked to other positive organizational outcomes, including increased creativity and appropriate risk taking (e.g., innovation; Sipe, 2016) and increasing ethical culture, moral agency of subordinates, and ethical leadership at lower organizational levels (Fehr, Fulmer, & Keng-Highberger, 2019; Schaubroeck et al., 2012).

1. Directly linking trust/trustworthiness and leadership constructs in this review, trust in leadership by subordinates has been linked to positive attitudes, behaviors, and performance outcomes in the workplace (Dirks & Ferrin, 2002). Is an effective way to build Insider TRUST through identifying and training leaders (and future leaders) in best leadership practices (e.g., demonstrating respect and valuing employees, setting and living up to organizational standards and expectations, clear communication)?
 - a. Several SMEs asserted that trust in leadership is related to loyalty to organizations and buy-in to organizational mission.
2. Changing and complex environments means that leadership requirements will change (see recent shift to *collective leadership research*, where leadership is studied as it is distributed across multiple members within an organization, e.g., Eva, Cox, Tse, & Lowe, 2019). What elements of best leadership practices will remain constant over time and what will need to change in order to retain our advantage in the human domain?

Sub-Constructs Linking Leadership and Trust/Trustworthiness

Integrity, Credibility, and Legitimacy

SMEs consistently linked these three constructs as key components of both trust (which is consistent with the literature) and good leadership (also consistent with the literature). Integrity is generally defined as, “consistency between word and deed, in line with a consistent set of principles or commitments, especially in the context of a temptation or challenge to the contrary,” (Worden, 2003, pp. 33). Legitimacy is the “generalized perception or assumption that the actions of an entity are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs, and definitions,” (Suchman, 1995, pp. 574). Credibility, and we use this as a research construct here rather than the specific operational meaning it has as part the security enterprise, refers to judgments made by a perceiver about the believability of the content and/or the communicator (O’Keefe, 2002). See Figures 3, 4, and 5 for the wide range of other constructs and factors in the literature related to integrity, credibility, legitimacy.

“Leaders who operate without integrity create environments where people feel they can do things they really shouldn’t. The integrity of the leader is critical to the integrity of the operating environment. Leaders demonstrate integrity by having a say-do ratio of 100% - if they say they’re going to do something, they follow through.”

SME #11

Figure 3: Integrity Construct Map – relationships to other constructs identified in the literature

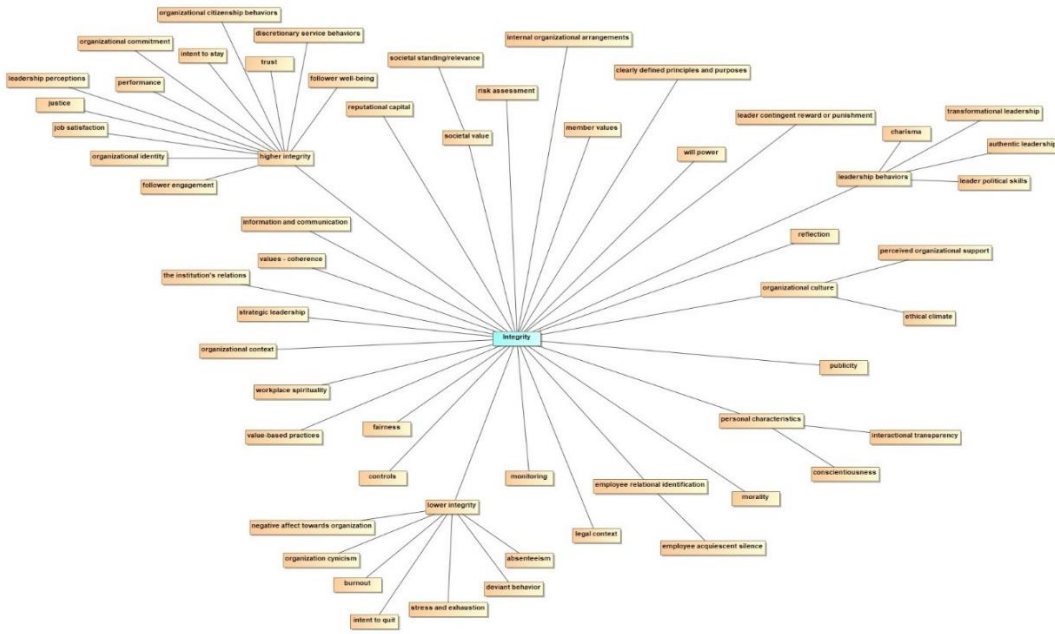


Figure 4: Credibility Construct Map – relationships to other constructs identified in the literature

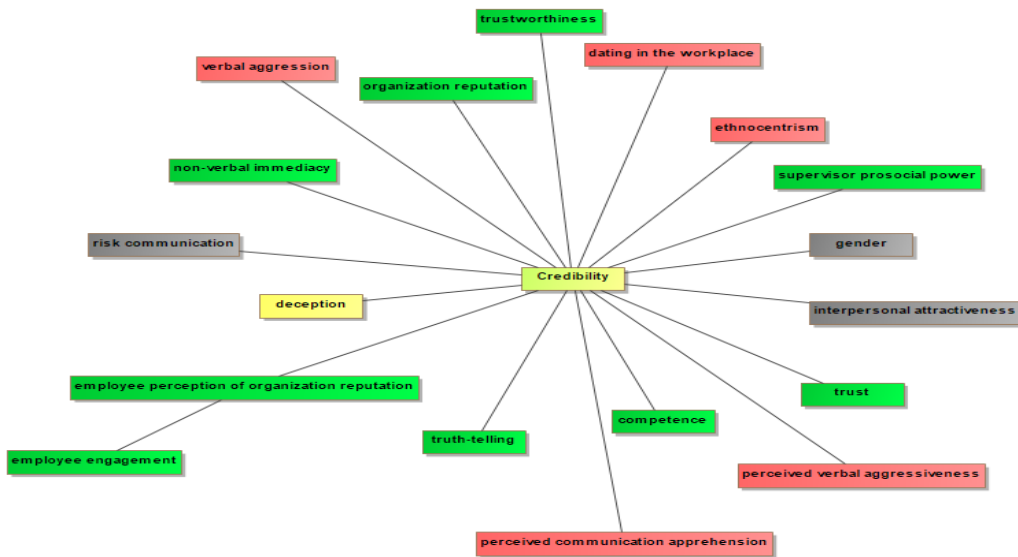
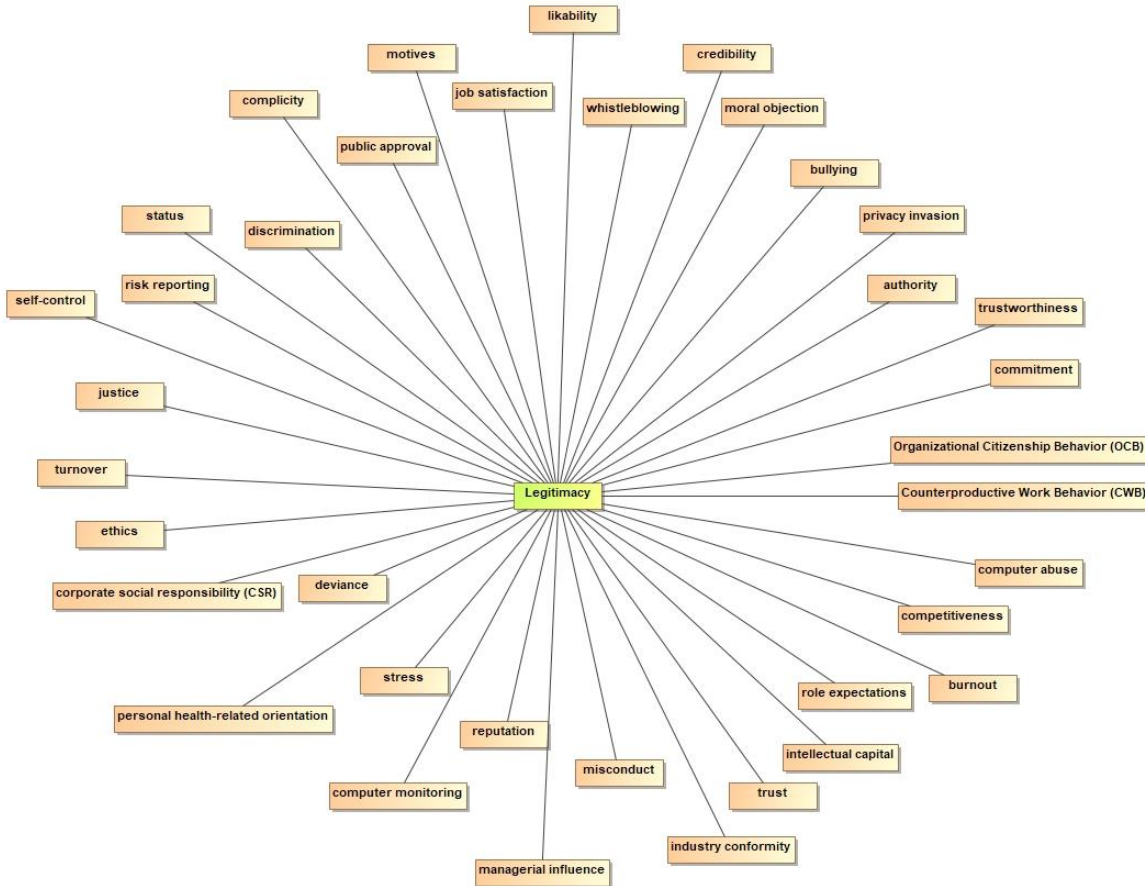


Figure 5: Legitimacy Construct Map – relationships to other constructs identified in the literature



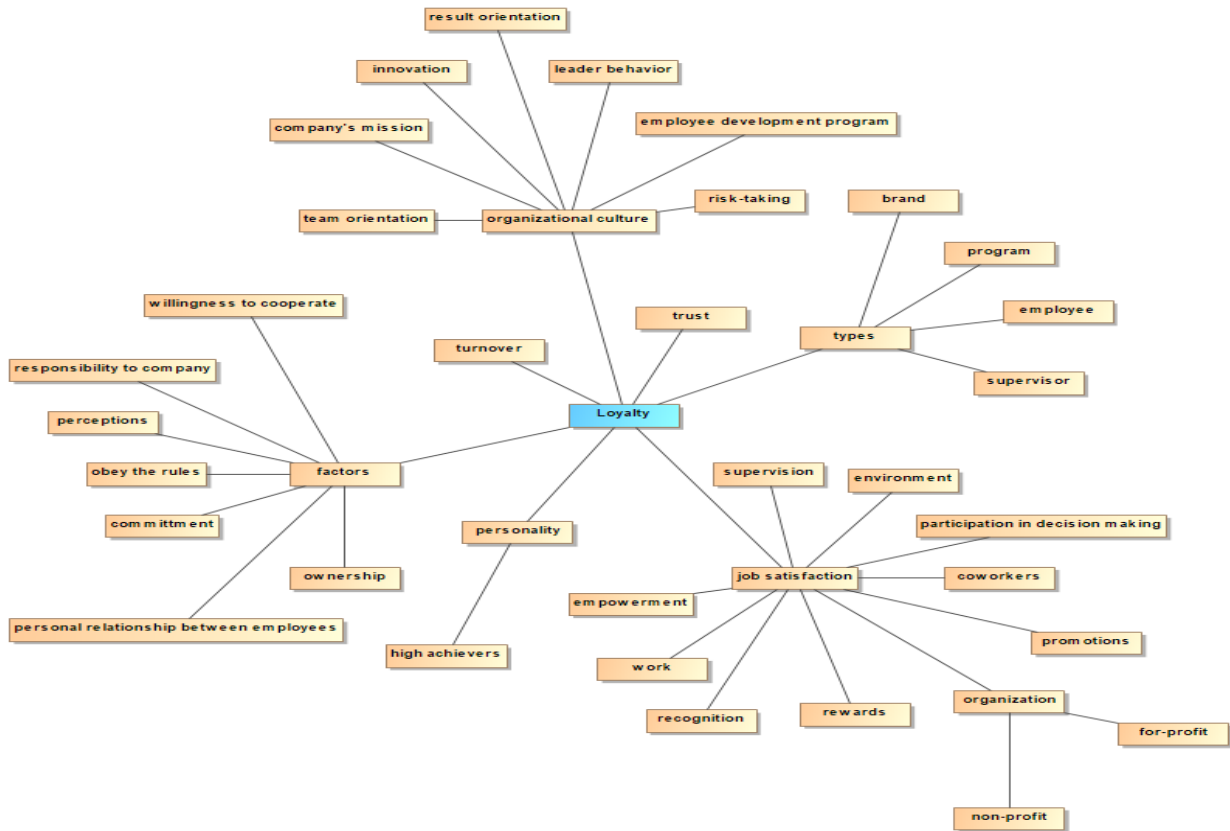
SMEs, particularly those with operational backgrounds, repeatedly stressed that while integrity, credibility, and legitimacy are difficult to assess (and define), they are not difficult to demonstrate to colleagues and subordinates. Further, consistently demonstrating integrity, credibility, and legitimacy is the best way to earn trust; while failing to live up to these standards is the fastest way to break trust.

1. Applied research question from SME: Can integrity be assessed effectively? If so, how can it be best incorporated in judgements of risk or trust?

Loyalty

SMEs referenced loyalty in many aspects, to organizations, to personal ideals, to missions, to colleagues, and to leaders. With our focus on loyalty in the workplace, we reference Powers (2000) definition of employee loyalty as multifaceted but centered around a fair exchange between the employee and their organization, such that the employee remains loyal to the organization so long as they see their contributions to the organization matched in what they receive in return from the organization. The input from the employee includes their time, expertise, adherence to company norms and remaining with the company. The organization must give back pay/benefits, recognition, job security, and sense of belonging, among other things (Powers, 2000). See Figures 6 for the wide range of other constructs and factors in the literature related to loyalty.

Figure 6: Loyalty Construct Map – relationships to other constructs identified in the literature



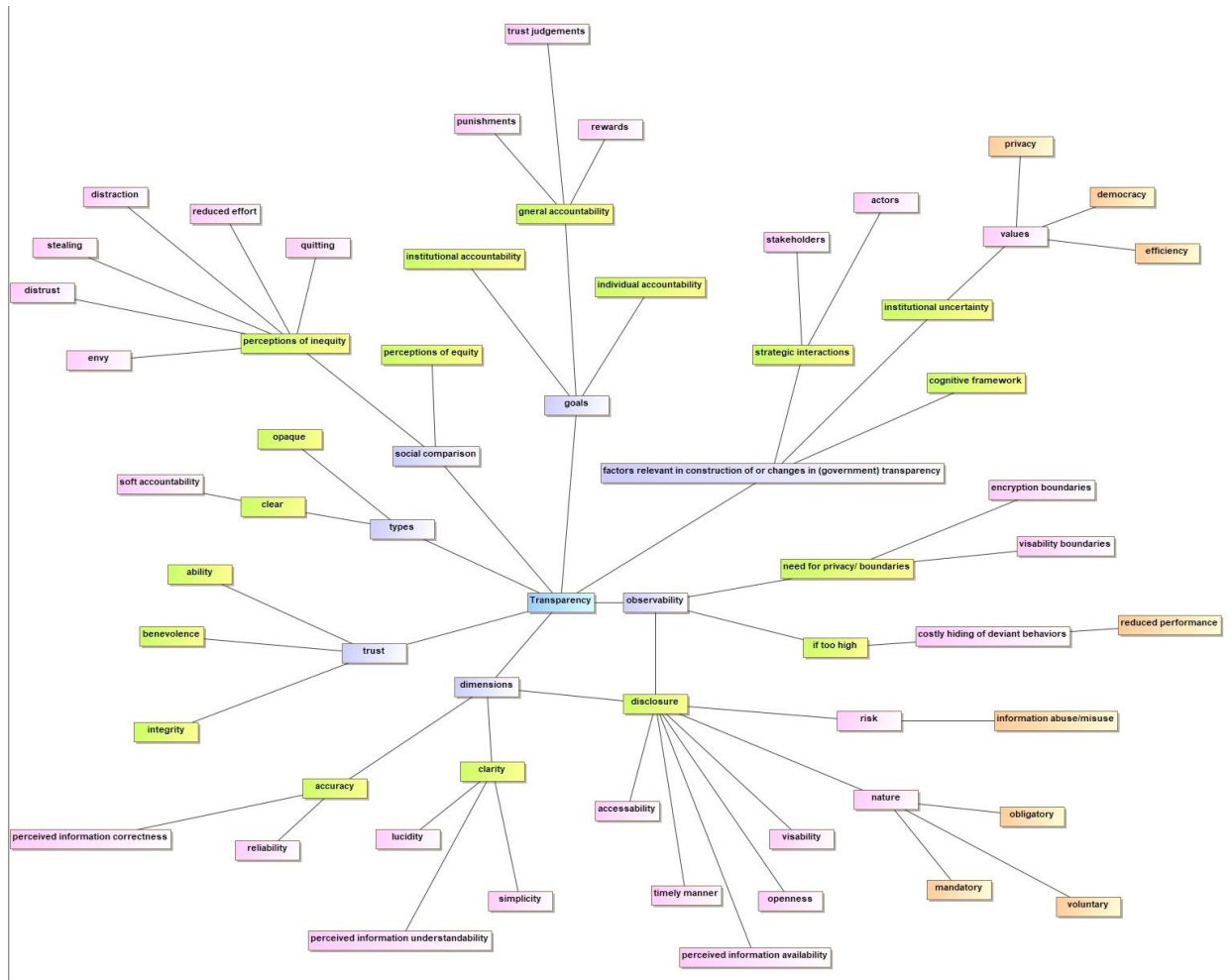
Two applied research questions from SMEs related to loyalty:

1. What kinds of loyalty (to different referents) are most important to building Insider TRUST?
2. While trust is a key factor in creating loyalty, what other factors (e.g., organizational supportiveness) create loyalty?

Transparency

SMEs raised two separate ideas regarding transparency, the “perceived quality of intentionally shared information from a sender,” (Schnackenberg & Tomlinson, 2016). First, transparency is an aspect of good leadership, as part of establishing communication. Several SMEs pointed out that lack of transparency can create mistrust in organizations, or create alienation when employees feel they are not valued or heard. See Figure 7 below for the wide range of other constructs and factors in the literature related to transparency.

Figure 7: Transparency Construct Map – relationships to other constructs identified in the literature



Second, and related, is that counter insider threat programs could benefit from greater transparency, especially regarding reporting concerns. Many are hesitant to report concerns to counter insider threat programs, often in part because they are worried about what will happen to their colleagues. Greater transparency regarding the rights and protections for individuals, when and how to report, and what support or resources are available for employees could all contribute to improving the perception of counter insider threat programs.

1. Applied research question from SME: What effect does greater transparency regarding the process of counter insider threat programs have on perceptions of the programs?

Group and Team Dynamics

“Good team dynamics can help mitigate risks of insider threats by preventing people from feeling alienated. Inclusiveness, good communication, and feeling like one has a voice are all part of the equation.”

SME #6

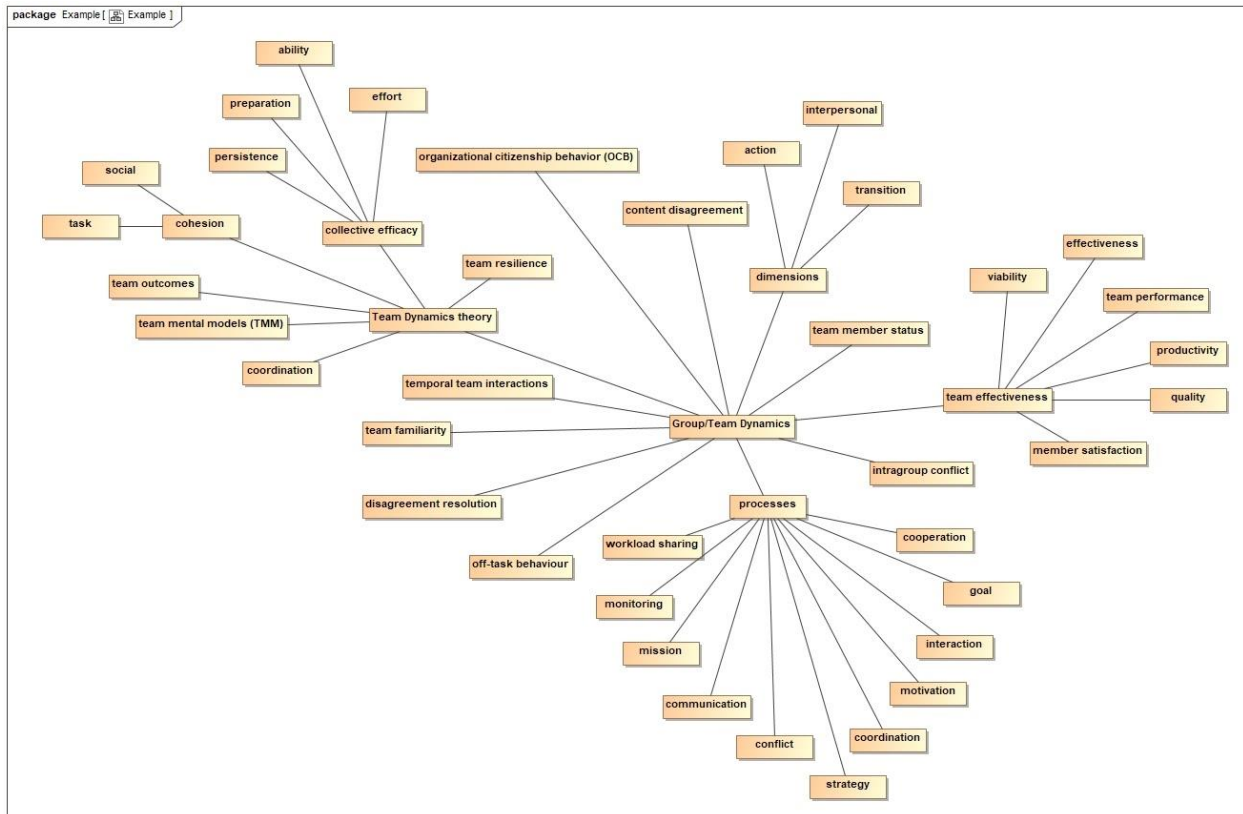
Group/team dynamics was considered to be somewhat important by most SMEs interviewed. Marks, Mathieu and Zacarro (2001) define team dynamics, “as members’ interdependent acts that convert inputs to outcomes through cognitive, verbal, and behavioral activities directed toward organizing taskwork to achieve collective goals.” Members carry out tasks independently that come together for the completion of a larger mission.

The field of group and team dynamics historically takes as systems level perspective to understanding social groups – positing that the group must be studied as a whole to be understood, rather than just be studying the individuals who make up the group (Hogg & Williams, 2000). Given the complexity of group and team dynamics, we highlight only a few key findings from the literature that are most relevant to building Insider TRUST here:

1. Group membership is a key aspect of individual social identity (Crano, 2000), thus closely identifying with a group is an important aspect of group bonds (see trust, leadership, and loyalty for further discussion)
 - a. Individuals have multiple group identities, which can sometimes conflict with one another
2. Group cohesion, or how closely members of a group are connected to one another, is closely linked to key behavioral outcomes of groups, including performance, conflict, and change (Forsyth, 2010)
3. Groups may have different structures, which may change over time as group needs change. These structures influence individual group members behavior, but are also influenced by the group members (Forsyth, 2009)

A theme that emerged from SMEs when discussing group and team dynamics was the importance of social connections within the workplace. As noted in the discussion above regarding leadership, the connection between employees and their direct supervisors, as well as to higher levels of organizational leadership, were stressed. However, SMEs also pointed out the value of strong peer level relationships between colleagues, and between individuals and their team(s).

Figure 8: Group and Team Dynamics Construct Map – relationships to other constructs identified in the literature



1. Applied research question from SME: what are the effects of respect and empathy on risks of different types of insider threat events?

Organizational Citizenship Behaviors and Counterproductive Workplace Behaviors

While our SMEs did not focus as heavily on these constructs in their interviews, they did generally rate both constructs as ‘most important’ without much elaboration. However, these constructs feature extensively in empirical literature from industrial/organizational psychology, management, human resources, and security, and show links to workplace performance (Dalal, 2005), productivity, turnover, and efficiency (Podsakoff, Whiting, Podsakoff, & Blume, 2009), and unethical decision making at work (Kish-Gephart, Harrison, and Treviño, 2010), suggesting it is an area worth exploring for possible applied research questions related to Insider TRUST. Organizational Citizenship Behavior (OCB) is “performance that supports the social and psychological environment in which task performance takes place” (Organ, 1997, p. 95). Counterproductive workplace behaviors (CWB) are any intentional employee behavior that is harmful to that organization (Gruys & Sackett, 2003).

However, several SMEs focused on the related construct of resilience, generally defined as, “(a) is a capacity that reflects in behavior; (b) deals with change; and (c) relates to overcoming some unwanted situation,” (Paul & Garg, 2012).

1. Applied research question from SME: how can we build trust and resilience throughout organizations to mitigate risk?
2. Applied research question from SME: are there impacts of technological advances on building resilience?
3. Applied research question from SME: does leadership making resilience a priority for their organizations decrease risks of insider events? Can leadership contribute to building individual employee’s resilience? Does individual resilience contribute to organizational resilience (and can that impact be measured)?
4. Applied research question from SME: can good leaders impact resilience by calibrating expectations of employees and team (in other words, by not overloading them with more than they can handle)?

Figure 10: Well-Being Construct Map – relationships to other constructs identified in the literature

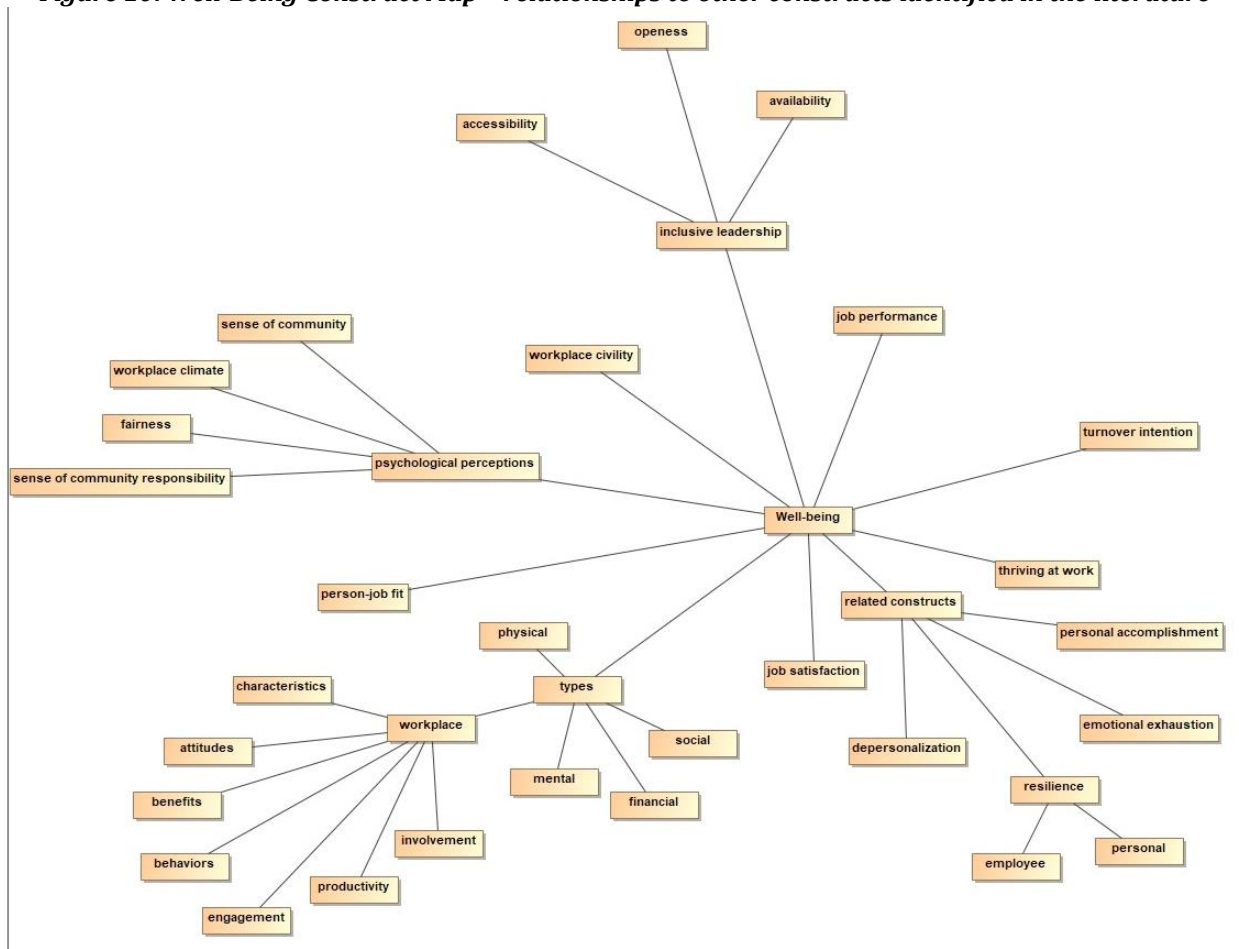
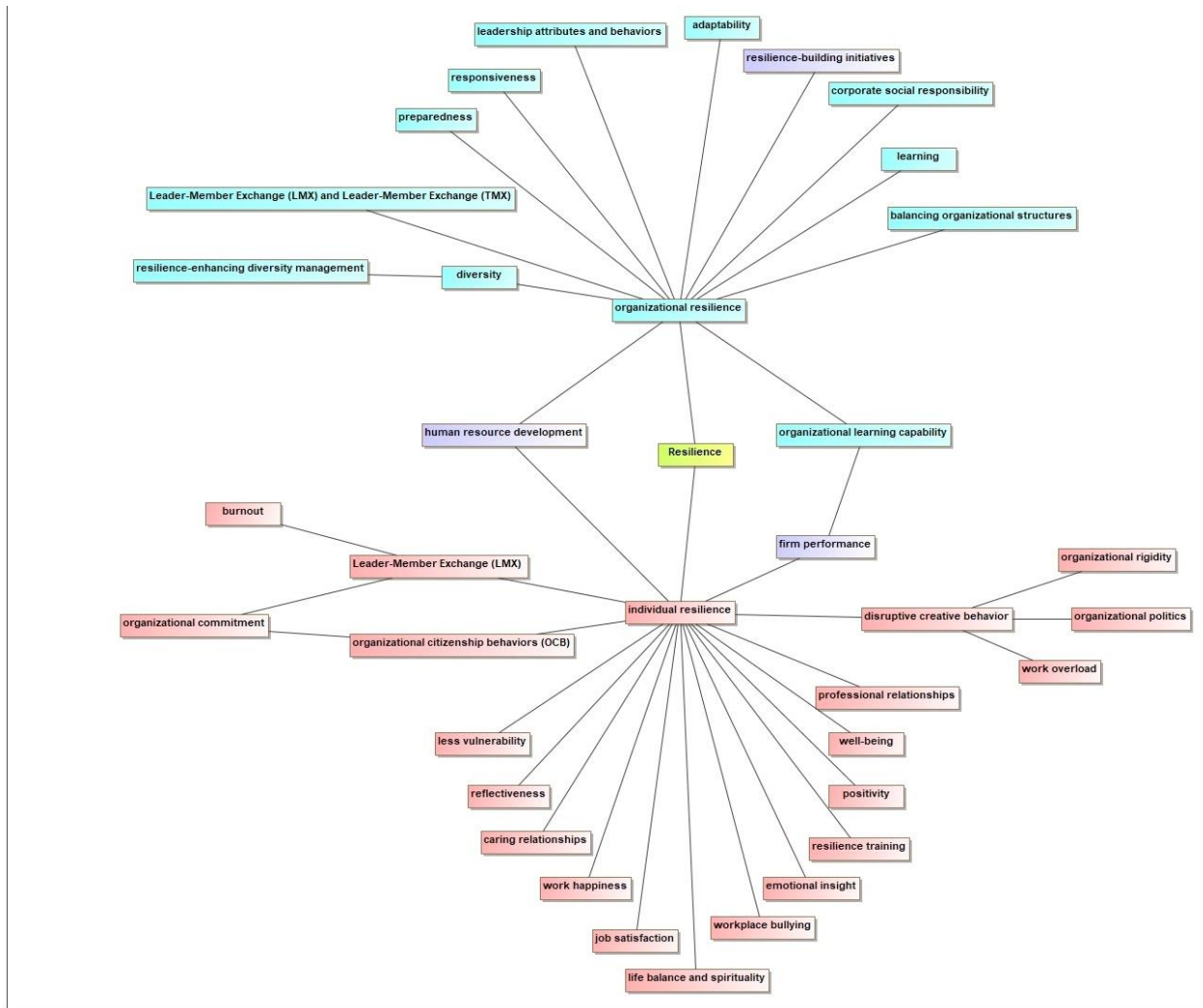


Figure 11: Resilience Construct Map – relationships to other constructs identified in the literature



Least Important Factors to Insider TRUST

The following factors were all ranked as ‘least important’ to developing Insider TRUST, but we included in the main report because they provoked strong negative responses for mitigating insider risk/threats. The majority of these factors center on the fixed or trait characteristics of individual (rather than the organization). Additional constructs we investigated but received little to no interest from SMEs included: incentives, courage, motivation, creativity, malevolent creativity, and burnout. See Appendix 1 for construct maps of all factors in this section.

Personality

Current research in insider risk/threat emphasizes individual characteristics such as personality as potential risk factors or indicators that an employee is becoming an insider threat (e.g., Greitzer, Kangas, Noonan, Brown, & Ferryman, 2013), in some cases even predictive of who will become insider threats (e.g., Basu et al., 2018). In conversations with SMEs, they significantly downplayed

the relevance and operational use of such data in mitigating insider risks/threats. One SME specifically highlighted the dangers in using such data as part of profiling or creating procedures, while another pointed out the mixed findings across the literature on the consistency of interpreting such data in a meaningful way. The only potential relevance identified to Insider TRUST was a suggestion that leadership training (see above) included training on recognizing and intervening with an individual's behavior became inconsistent with their individual norms in a concerning way.

There are several models of personality, mostly drawn from psychology research, the most well-known and well used are the Big Five (McCrae & Costa, 1987) and the HEXACO model (Ashton & Lee, 2008) which is an extension of the Big Five. The Big Five scale assess individual's personality traits on a sliding scale (low to high), with most scoring somewhere between the extremes, on extraversion (outgoingness), agreeableness (friendliness), neuroticism (temperamentality), openness (curiousness), and conscientiousness (discipline). HEXACO uses a similar assessment, though it terms neuroticism as "emotionality" and adds a sixth factor of honesty-humility. Other models include the Dark Triad, which comprises narcissism, Machiavellianism, and psychopathy and generally indicates malevolence (Paulhus & Williams, 2002). Then there is the Light Triad, which comprises humanism, Kantianism, and faith in humanity (Kaufman, Yaden, Hyde, & Tsukayama, 2019).

Individual Difference Factors & Optimism

In addition to personality, discussed above, individual difference factors can include optimism (which we initially included as its own construct for consideration), explanatory style, locus of control beliefs and self-efficacy, interest, and aptitudes. SMEs downplayed these other factors even more so than personality. The only comment made, by one SME, was that some individual difference factors can cause divisions in the workplace, but not if appropriately managed by good leaders, and that they did not see much operational value in collecting data on these factors.

Optimism is generally defined as holding generalized expectations for the future (where positive expectations make one an optimist, negative expectations make one a pessimist). As with personality, there are several theories, but widely accepted is Carver, Scheier, and Sergerstrom (2010) quoted above. Explanatory style, locus of control beliefs, and self-efficacy are highly inter-related, and describe how individuals attribute cause of events (explanatory style; Alloy, Peterson, Abramson, & Seligman, 1984), where control over events resides – internal to the self or external to the self (locus of control; Rotter, 1966), and how much control they have over events (self-efficacy; Bandura, 1982). Optimism, explanatory style, internal locus of control, and high self-efficacy are generally linked to positive outcomes such as subjective wellbeing and developing coping strategies (Peterson & Steen, 2009).

Subject Matter Expert Interviews

Following our review of the literature, we developed a semi-structured interview protocol designed to elicit feedback on our proposed Insider TRUST constructs, additional constructs to be included, as well as potential relationships between these constructs. The semi-structured interview format allowed for back-and-forth conversation regarding the interviewee's expertise and opinions regarding important questions that should be addressed in future research. The goal of the literature review in combination with the SME interviews was to 1) identify common themes and questions among insider threat operators, researchers, and policymakers, 2) develop, refine, and expand the conceptual model of relevant constructs, and 3) develop future operationally focused research questions related to the larger program of research on insider risk/threat at ARLIS.

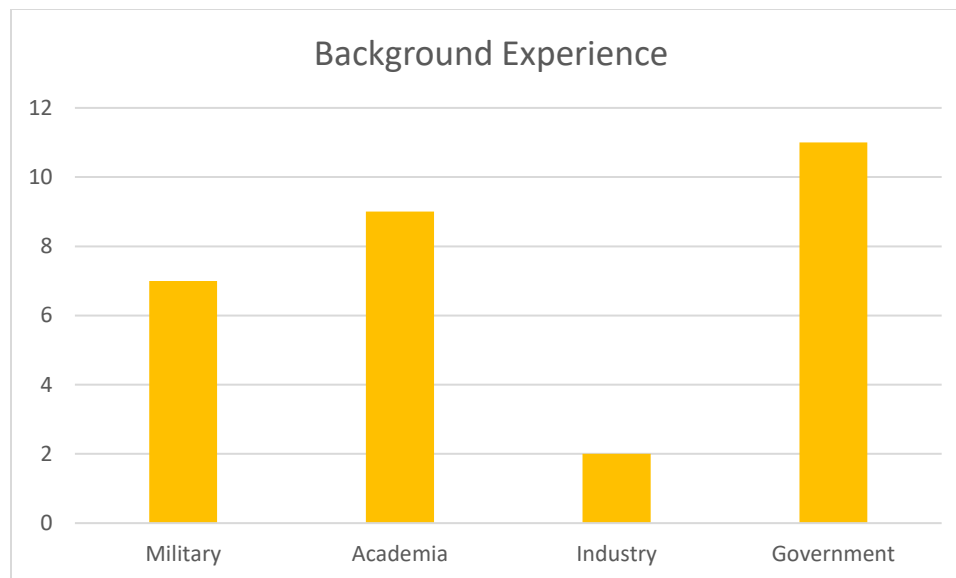
Methods

Exempt human subjects research to carry out interviews were obtained by the University of Maryland Institutional Review Board (UMD IRB) and the Office of Research Protections, U.S. Army Medical Research and Development Command. The goal of these interviews was to 1) identify common themes and questions among insider threat operators, researchers, and policymakers, 2) refine and expand the conceptual model of relevant constructs, and 3) develop future research questions related to the larger program of research on insider threat at ARLIS.

Participants

We conducted interviews with a total of 12 insider threat subject matter experts, in addition to two internal pilot interviews with colleagues who are also insider threat SMEs, between June and August 2021. Participants were identified through ARLIS' principal investigators for Insider TRUST, the assistance of the government program manager, and recommendations from interviewed participants. Table 1 shows the participant break-down of background experience by military, academia, industry, and government. All participants had experience in at least two fields. 7 participants interviewed had background experience with the military, 9 participants interviewed had background experience in academia, 2 participants interviewed had background experience in industry, and 11 participants had background experience in government.

Table 1. Background Experience of Subject Matter Experts



Procedure and Interview Protocol

After participants were recognized as subject matter experts (SMEs) in insider risk, invitations for a one-hour interview were sent out. Once participants confirmed the day and time of the interview, they were sent the list of interview questions, construct list A or B, and 5 randomly selected construct maps associated with the overall construct list. Construct lists A and B were created because of the large number of constructs our team identified and were the list of constructs randomly halved and then randomly given to participants.

Data Analysis

Data was coded by ARLIS researchers with a team of undergraduate and graduate interns for the summer using a qualitative approach. Content analysis was used to quantify repeated constructs, ideas and actions to identify major themes from each interview question.

Question 1. Background experience of our SMEs.

We were not interested in an SME's title but the SMEs' background experience within the insider threat realm. Background experience was broken down into whether an SME interviewee currently or previously worked in military, academia, industry, or government related areas within insider threat.

Question 2. The 5 most important Insider TRUST constructs.

The goal of this question was to ask SMEs to generate their own constructs before looking at our construct list so that they were not constrained by our preconceived notion of important Insider TRUST constructs. Each construct identified by the SME was sorted by constructs already identified by the ARLIS research team for a baseline literature review and constructs that had not been selected for the literature review. Constructs were also separated by internal (or individualist), external (environmentally related), social groups and relationships, and other associated themes mentioned with the construct identified.

Question 3. Ranked ARLIS constructs.

Each participant received a randomly generated list of half the total constructs identified (Construct List A or B) as relating to Insider TRUST. Once the SME identified each construct as most, somewhat, or least important constructs relating to Insider TRUST, then participants were asked to provide an explanation as to why they chose that category for the particular construct. When SMEs were unaware of the definition for a particular construct, they were provided with the ARLIS researcher's definition. (See Appendix 2) SMEs were also able to suggest additional constructs they felt were missing from the list provided to them.

Question 4. Best ways to mitigate insider risk.

SMEs were asked to share positive ways to mitigate risk based on their past and current experience. Responses were coded into actions, construct, area of research, or other as pathways to mitigate risk. The action category is where SMEs suggested approaches to responding to mitigating risk. Actions could involve training, relationship-building, both or neither. Actions were also identified as either referring to leadership, personnel, both or neither. A term, idea or concept made up the construct category. Constructs were identified as either being constructs originally identified by ARLIS researchers or not. Area of research was defined as a process that was usually stated as a question or statement describing gaps in literature. Finally, 'other' was used to place best practices that didn't seem to fit into any of the other categories. This question also captured ideas and constructs of what not to do to mitigate insider risk.

Question 5. Future research

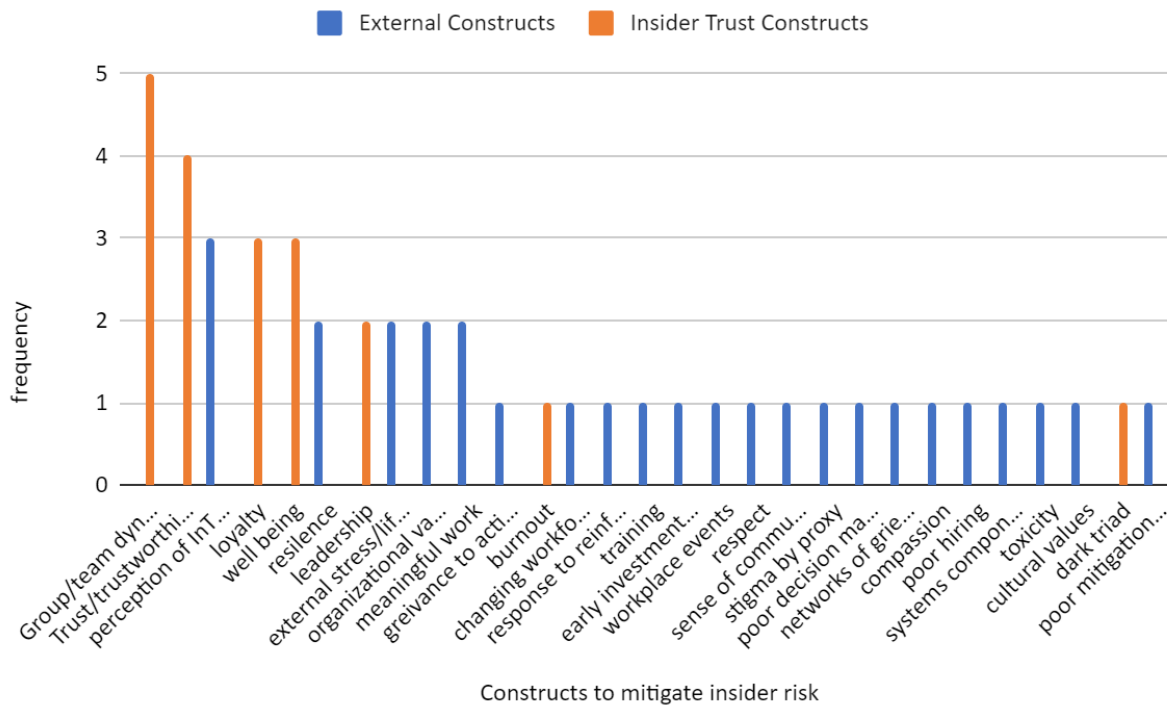
This question was important for collecting SME's future research questions that usually focused on areas where they would like to see more research on or gaps in the research or current practices.

Results

Q2. The 5 most important Insider TRUST constructs.

While we asked for five of the most important Insider TRUST constructs, there were some SMEs that listed less than and more than 5 constructs. We were able to identify a total of 29 constructs from the 12 SMEs which can be found in Table 2 that shows the construct named and the frequency SMEs mentioned that construct. Of the total Insider TRUST constructs provided, 7 matched our list of constructs (sent to them ahead of the interview), while 22 were unique constructs (not on ARLIS construct list).

Table 2. Most important Insider TRUST constructs.



Teamwork

Teamwork was identified most frequently as an important Insider TRUST construct by SMEs interviewed. SMEs identified the importance of “positive and noncritical relations between coworkers and supervisors,” as well as the importance of “identifying how ostracization, ideologies, and external motivations can lead to Insider Threat behaviors (e.g., Chelsea Manning). Employees feeling like they have a voice and are included in [their] organization is very important in this respect.”

Trust/Trustworthiness

Trust/trustworthiness was the second most frequently identified Insider TRUST construct by SMEs interviewed. SMEs mentioned that “many employees are unsure if they are valued or trusted by their organization. Disgruntled employees and those that feel ostracized/not appreciated by the organization may retaliate against the organization.” SMEs also mentioned the importance of “building trust by demonstrating competence, caring, [and] integrity.”

Perception of Insider TRUST

Perception of Insider TRUST was tied with Loyalty and Wellbeing as the third most frequently identified Insider TRUST construct by SMEs interviewed. This construct was a distinctive construct not contained in ARLIS’ current literature review. SMEs considered the perception of Insider TRUST as viewing “people as assets do not threat [which required organizations and members concerned with insider risks to] safeguard [their] assets.” Furthermore, our SMEs argued that carrying out

investigations should “look for confirming and disconfirming evidence, hold investigators responsible for explaining determinations and help reduce bias [by] promot[ing] justice.”

Loyalty

Loyalty, which was identified by SMEs, was also identified by the ARLIS research team. SMEs pointed out that loyalty could “probably [be] very strong in small organizations and very difficult to quantify in large organizations.” Others looked at how to achieve loyalty noting that “punishment does not engender loyalty, whereas rewards do. [It is important to] think about employees’ entire work cycle and their needs.”

Well-being

Well-being, which was identified by SMEs, was also identified by the ARLIS research team. SMEs referred to well-being as the mental health/happiness of employees in addition to the balance between wellness and accountability. SMEs mentioned that well-being was a ‘human construct’ that was a ‘component of burnout’ and related to traits defined in the dark triad and stress. One SME mentioned that “happy people don’t betray [the] interests of [their] organization.”

Resilience

Resilience was tied with Leadership, External stress/ life events, and Organization as the fourth most frequently identified Insider TRUST construct by SMEs interviewed. This construct was also identified by the ARLIS research team for our literature review. SMEs referred to resilience as an approach that factored in variables of risk, vulnerabilities and consequences of organization and employee behaviors.

Leadership

Leadership was also identified by the ARLIS research team as a sub-component of C-Suite. SMEs mentioned that there needed to be a commitment from leadership to establish a risk management framework, include people in that framework, to remain active in organization, know the goal and culture of an organization and be able to know when employees did not align with the goals and culture of the organization.

External stress/life events

External stress/life events were a distinct construct from the ARLIS identified constructs. SMEs mentioned that personal events external to work, usually involving family can cause stress. Other SMEs were interested in possibly researching the correlation of environmental factors that led to insider risk behaviors, noting that Wall Street is an extremely unhealthy working environment but tends to have less insider risk events than those occurring within the government sector.

Organization

Organization was a unique construct identified by SMEs and included the following sub-components: perceived organizational support, organizational justice, performance-based rewards and recognition, direct supervisor support, organizational communication, employee engagement, coworker connectedness, and ensuring] employee is in line with organization.

Other constructs

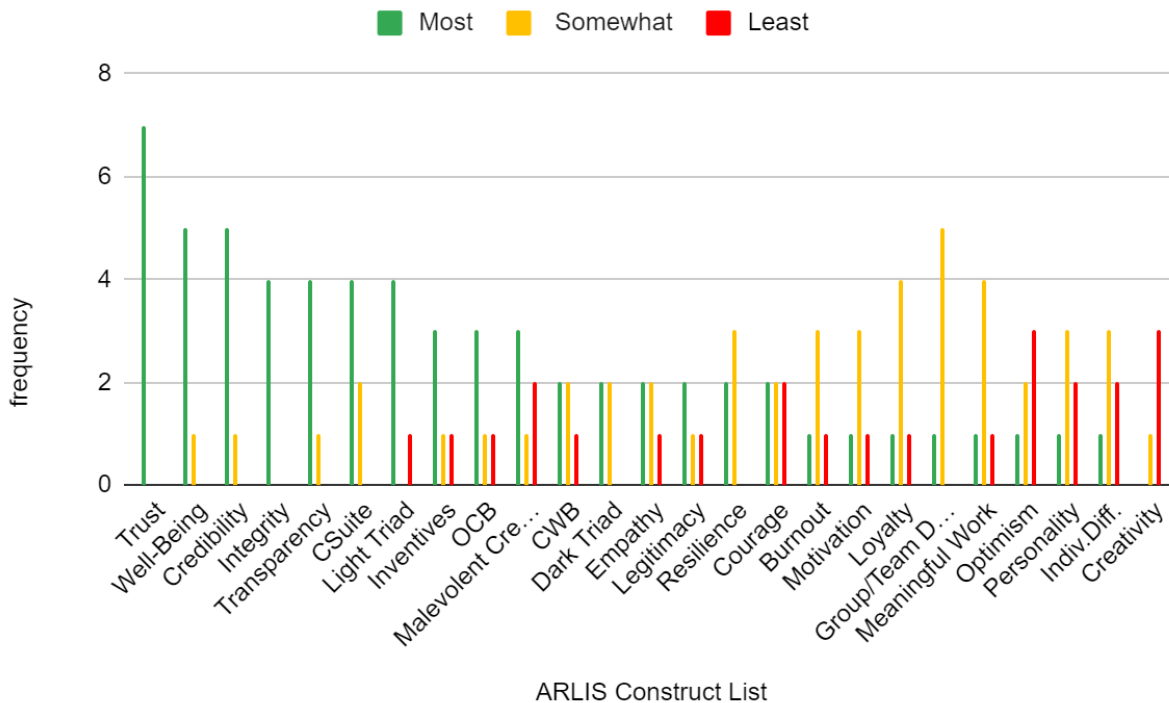
These remaining constructs were mentioned once by SMEs as being important. ARLIS had also identified these two constructs as part of their literature review: burnout and dark triad. The following 17 constructs were unique Insider TRUST constructs: grievance to action (pathway to

violence), changing workforce, response to reinforcement vs punishment, training, early investment in personnel, workplace events, respect, sense of community, stigma by proxy, poor decision making/critical thinking, networks of grievance, compassion, poor hiring, systems component, toxicity, cultural values, and poor mitigation management.

Q3. Ranked ARLIS constructs.

After asking SMEs about the constructs, they considered the most important to mitigating insider risk, we followed up by asking participants to look at a randomly selected list of half the constructs ARLIS researchers identified. With this list, SMEs were asked to rank the order of constructs presented to be most, somewhat, or least important and the results can be seen in Table 3. The top-ranking most important constructs were Trust (7 SMEs), Well-being (5 SMEs), Credibility (5 SMEs), Integrity (4 SMEs), Transparency (4 SMEs), C-Suite (4 SMEs), and Light Triad (4 SMEs). The dominant somewhat important constructs were Group/Team Dynamics (5 SMEs), Loyalty (4 SMEs) and Meaningful Work (4 SMEs). The leading constructs identified as least important were Optimism (4 SMEs) and Creativity (4 SMEs). Discussion of constructs are based on the frequency with which SMEs identified them as most important.

Table 3. Ranked ARLIS constructs by most, somewhat and least importance



Trust

Seven total SMEs mentioned that Trust is one of the most important constructs in Insider TRUST. This number also included SMEs who identified Trust as a construct not on their randomly selected list but still very important. One SME mentioned that Trust is cross-cutting along manager-employee's relationships, organizational culture, philosophy and helps employees to identify where they fit into an organization. Furthermore, another SME noted that, "if people feel trusted, most people will want to live up to that trust." Establishing ways for individuals to trust the organization can be positive and build loyalty.

Well-being

Six SMEs rated Well-being (5 ranked Well-being as most important, one ranked as somewhat important). SMEs mentioned that it was important for employees to be able to cope with stress positively and that there needed to be a balance between well-being and catching bad guys. "Happy people don't betray [their organization]." Several theories were mentioned that included self-determination theory, critical path theory and Calhoun threat assessment model.

Credibility

Six SMEs rated Credibility (5 ranked Credibility as most important, one ranked as somewhat important). Five out of the six SMEs believed that Credibility is directly correlated with trust and trustworthiness. If a person, leader, or organization is not perceived as credible then there is no foundation for trust.

Integrity

Four total SMEs all ranked Integrity as the most important construct in Insider TRUST. SMEs mentioned that legitimacy and ethics are entwined with integrity and cannot be achieved until integrity has been established. All of these constructs come together to achieve transparency, communication, and trust. Leadership was brought up along with this construct and SMEs noted that "Leaders without integrity create environments where people feel they can do things they shouldn't." Social movement theory was mentioned as a way to measure unrest when expectations don't meet reality.

Transparency

Five SMEs rated Transparency (4 ranked Transparency as most important, one ranked as somewhat important). SMEs had noticed that transparency comes with clear communication, establishing a common goal and that a lack of transparency increases mistrust among stakeholders.

C-Suite

Six SMEs rated C-Suite (4 ranked C-Suite as most important, 2 ranked as somewhat important). SMEs stressed the importance of active leadership, leadership taking ownership of policies and programs, and then setting an example by following organizational policies and programs. A lot of research focuses on the upper echelon of leaders in organizations, but SMEs mentioned that middle managers may be more important because they interact with employees more.

Light Triad

Six SMEs rated Light Triad (4 ranked Light Triad as most important, one ranked Light Triad between most and somewhat important, one ranked as least important). Most SMEs mentioned that these elements in the Light Triad are important for leadership and may increase well-being at work

and the possibility for employees to experience meaningful work. Other SMEs believe that these traits are important to minimize insider risks. While one SME did not believe that personality information was important or could be used as operational data.

Incentives

Five SMEs rated Incentives (3 ranked Incentives as most important, one ranked as somewhat important, 1 ranked as least important). Some SMEs agreed that incentives could positively motivate the workforce. However, other SMEs mentioned that some incentives could have a negative effect by not considering that some people would like social recognition or are mission driven and would benefit more from outcomes rather than incentives.

Organizational Citizenship Behaviors (OCB)

Five SMEs rated Organizational Citizenship Behaviors (OCB) (3 ranked OCB as most important, one ranked as somewhat important, one ranked as least important). Few SMEs followed up with an explanation on this construct. The SMEs that did explain their choice to rate OCBs believed that this construct was instrumental in allowing people to behave and express themselves using constructive strategies to cope with stressors.

Malevolent Creativity

Six SMEs rated Malevolent Creativity (3 ranked Malevolent Creativity as most important, one ranked as somewhat important, 2 ranked as least important). Responses to malevolent creativity were split. Two SMEs suggested that creativity of any kind was important while others noted that malevolent creativity was bad for an organization and increased threats.

Counterproductive Workplace Behaviors (CWB)

Five SMEs rated Counterproductive Workplace Behaviors (CWB) (2 ranked CWB as most important, 2 ranked as somewhat important, one ranked as least important). Several SMEs mentioned that these are not normal behaviors and would be indicators of threats detected in a risk management framework.

Dark Triad

Four SMEs rated Dark Triad (2 ranked Dark Triad as most important, 2 ranked as somewhat important). SMEs unanimously agreed that people who exhibited these traits were at high risk for engaging in insider threats or causing others to engage in risk behaviors.

Empathy

Five SMEs rated Empathy (2 ranked Empathy as most important, 2 ranked as somewhat important, one ranked as least important). Interestingly, all SMEs noted that empathy was necessary for people to feel connected, valued, and safe. Some SMEs mentioned that empathy was a subcategory of trust. One SME claimed that empathy is a perceived term and important perceived outcome while another stated that empathy plays an important role in negotiation, managing risk and building relationships.

Legitimacy

Four SMEs rated Legitimacy (2 ranked Legitimacy as most important, one ranked as somewhat important, one ranked as least important). Two SMEs ranked legitimacy as it relates to employee/manager relationships, with one SME reporting their dislike for the term but the importance for building bonds between supervisor and subordinate relationship. Other SMEs noted

that while this is less important than other constructs there are connections between legitimacy and trust and increased loyalty.

Resilience

Five SMEs rated Resilience (2 ranked Legitimacy as most important, 3 ranked as somewhat important). SMEs agreed that resilience prepares people and organizations for stresses and is a positive attribute. However, most SMEs mentioned that this was not the most important construct and that, “if you have established trust, properly incentivized employees, and motivated the workforce, then you have complete transparency. In this case, resilience is not needed because the workforce is going to behave appropriately with or without it.”

Courage

Six SMEs rated Courage (2 ranked Courage as most important, 2 ranked as somewhat important, 2 ranked as least important). Courage seemed to be evenly split across the ranking categories. One SME who believed it to be most important mentioned that it takes courage to report insider threats; while another SME mentioned that for them personally it was very important but doubted that other SMEs they have come in contact with would feel the same. The remaining SMEs remained apathetic to this construct, one citing that there are too many definitions for this construct to be useful in the insider realm.

Burnout

Five SMEs rated Burnout (1 ranked Burnout as most important, 3 ranked as somewhat important, 1 ranked as least important). SMEs linked Burnout to not caring any more, to the inability to handle stress and being psychologically overwhelmed which leads to people behaving outside of how they normally would.

Motivation

Five SMEs rated Motivation (1 ranked Motivation as most important, 1 ranked as somewhat important, 1 ranked as least important). One SME connected motivation to incentives and burnout. Two SMEs mentioned that generating motivation was the responsibility of managers and organization. Other SMEs mentioned that this was not very important as an indicator of risk.

Loyalty

Six SMEs rated Loyalty (1 ranked Loyalty as most important, 4 ranked as somewhat important, 1 ranked as least important). Several SMEs had difficulty defining this construct and mentioned that it was hard to measure. Other SMEs believed that problems arise when an employee does not see themselves aligning to the organization which can cause adverse effects. While organizational supportiveness creates loyalty among employees.

Group/Team Dynamics

Six SMEs rated Group/Team Dynamics (1 ranked Group/Team Dynamics as most important, 5 ranked as somewhat important). SMEs overwhelmingly considered this a somewhat important construct. “Good team dynamics help minimize in[sider] risk by preventing people from feeling alienated. Inclusiveness, communication, and feeling like one has a voice are important.” Other SMEs noted that active leadership is also important in mitigating problems within teams, in addition to the relationship between a supervisor with perceived close connection to the organization and their subordinates.

Meaningful Work

Six SMEs rated Meaningful Work (1 ranked Meaningful Work as most important, 4 ranked as somewhat important, 1 ranked as least important). Overall, SMEs did not consider this an important motivator in insider risk but could be linked to loyalty within an organization, work ethic, and well-being.

Optimism

Six SMEs rated Optimism (1 ranked Optimism as most important, 2 ranked as somewhat important, 3 ranked as least important). SMEs mostly dismissed Optimism, but some did note that it can be beneficial in an organization or leadership, especially during a crisis.

Personality

Six SMEs rated Personality (1 ranked Personality as most important, 3 ranked as somewhat important, 2 ranked as least important). SMEs mostly believed that personality research should not be as influential as it is with one SME suggesting that the Big Five be thrown out to another SME commenting that personalities do not solely determine skills and traits of a person within an organization.

Individual Differences

Six SMEs rated Individual Differences (1 ranked Individual Differences as most important, 3 ranked as somewhat important, 2 ranked as least important). A couple of SMEs mentioned that this is a big space for research that can go wrong if done incorrectly. Especially profiling people based on their personality rather than their behaviors. One SME mentioned that “Individual differences can cause divisions in organizations (such as political differences). They must be managed [by leadership] to avoid friction in workplace.”

Creativity

Four SMEs rated Creativity (1 ranked Creativity as somewhat important, 3 ranked as least important). Most SMEs found this construct to be least important. One SME mentioned that “creative people can be risky but stifling creativity can be counterproductive. One SME suggested that most people will change their environment if they are unhappy with their current circumstances.

Q4. Best ways to mitigate insider risk.

We asked SMEs what best ways were to mitigate insider risk and/or build Insider TRUST. SMEs identified ways to address these best practices through action (28), constructs (4), areas of research (3) and 1 one idea that fell outside of the other 3 categories.

Actions

There was an overwhelming consensus among SMEs that actions to and from leadership (senior and middle management) would address best practices. Three sub-categories under leadership included building up leadership skills, communication, and caring. SMEs mentioned that training for leadership should begin early and consistently over time. One SME mentioned that supervisors should be competent in their assigned roles and that there should be, “a way of implementing checks and balances on supervisors once they are in place.” SMEs believe in the importance of leaders who are able to express their intentions. “Leaders should communicate objectives, methods

to complete objectives, and individual expectations so as to empower employees to achieve organizational goals.” Several SMEs mentioned that those in leadership positions should be respected, thoughtful and caring no matter their position. Showing support and kindness built up loyalty among employees. Furthermore, it is leadership’s responsibility to develop organizational culture and to intervene when other employees or leaders’ behaviors were out of line. Leadership should have engagement skills to be able to lead and manage people but that would also allow them to understand subordinates’ behaviors because they are responsible for the actions of their employees.

SMEs also identified that changes in hiring practices should occur to ensure that people are best suited for the organization and align to the mission of the organization. Furthermore, after onboarding new personnel, “Organizations should provide training on reporting procedures and clearly convey what the expectations and responsibilities are of all employees, including obligations involving non-disclosure agreements.” SMEs also stressed the importance of insider threat programs. This included circulating a positive perception of Insider Trust programs through wellness stories, fostering an environment where people are comfortable reporting, demonstrating competence and responsibility to inspire people to speak up against unacceptable behavior, and encouraging employees to report when they feel that something is off rather than try to prove it themselves. Other actions mentioned less frequently included trust, awards, and recognition, fostering team dynamics, protecting privacy, and addressing investigation practices.

Constructs

SMEs mentioned these constructs: Compassion as it relates to leadership, respect among teams, and risk management. One SME mentioned that compassionate leaders foster a positive work environment by showing compassion to employees in the organization. An organization’s mission should be above the welfare of the employees. An organization’s mission should not be above the well-being of its employees. Respect within teams was mentioned as, “the best violence prevention approach” and referred to old fashion kindness, caring about each individual, and working together collectively. Risk management dealt with both mitigating bad things but also revealing good ideas as well.

Areas of Research

SMEs identified areas of research for mitigating risks by asking questions regarding how much an organization is responsible for its employees, what level of involvement an organization can engage in with employees without overstepping the privacy of those employees, and when an organization can determine what behaviors are risky enough to intervene. Other SMEs were interested in studying the point of view of perpetrators, bystanders/bystanders of bystanders, and supervisors as they relate to unacceptable behavior.

Other

A permeating idea that did not seem to fit in the previous categorizations of mitigating risks was the idea that people are assets rather than threats and that organizations should find ways and tools to safeguard those assets. Organizations should be giving positive reinforcement rather than punished.

Finally, SMEs mentioned some tactics that would not work in mitigating risk. As it relates to insider programs, SMEs suggested not acting in an intimidating or suspecting manner or jumping to solutions without understanding the problem first. Humiliation was mentioned a couple of times as being a trigger for people to do something bad. Finally transferring people who have been found engaging in risk behavior is unacceptable in addition to toxicity in middle management.

Q5. Future Research

Questions and areas of future research were collected from SMEs and can be found in Table 4. SMEs brought up a large number of questions about current Insider TRUST. This included how threat is being defined now, what tools can help to preempt threat (risky) situations, what skills are necessary for leadership to interact with employees to decrease Insider risks and how to manage insider threat at all levels of government because a one-size-fits-all approach is not working. Some SMEs pointed to the lack of theoretical models and suggested researching alternative models from other disciplines (game theory, I/O, leadership, communication, risk-based decision-making) to adopt or modify in addition to identifying the variables needed for a risk model. Another idea that was mentioned frequently was trust. This included how to build trust in leadership, organization, and insider programs.

A couple of SMEs referred to resilience, behavior, case studies and effectiveness of mitigating insider risks. Some areas of research around resilience looked at how to build up trust and resilience in organizations to anticipate threats and what the impact and side effects are of technological advances on individual resilience. SMEs wanted to know what the connection was between external factors and the workplace and their relation to behaviors; in addition to researching best practices to address problematic or disruptive behaviors. Other SMEs also mentioned the importance of having applied approaches through case studies rather than abstract research to help various audiences understand and become interested in this problem.

These remaining areas for further research were mentioned once by SMEs as being important. ARLIS had also identified these seven constructs as part of their literature review: Dark Triad, Empathy, Individual Differences/Personality, Integrity, Loyalty and Motivation. The following 12 concepts were unique areas of research: Balance (organizational vs individual), role of bystanders in reporting, contribution of disinformation to future threats, shelf life of indicators, meaningful work, respect, does people's sense of social justice steer them to engage in risky behaviors, understanding triggering events, what tools are necessary to mitigate risk, how should positive and deterrence practices get validated and is there a way to value culture and individuals within organizations.

Table 4. Questions suggested for future research

balance	How do you balance individual and organizational concerns?
---------	--

behavior	<p>What is the empirical connectivity between workplace and external factors on ultimate behavioral outcomes?</p> <p>How do you address those potentially problematic/disruptive behavioral characteristics?</p>
<hr/>	
bystanders	<p>What is the role of bystanders and bystanders of bystanders in reporting InT?</p>
case studies	<p>Do in depth case studies of organizations that created conditions/policies that we and others believe led to lower levels of risk; and organizations that led to higher risk; ask interdisciplinary group to go through that and see what they thought was critical.</p>
CInT	<p>What tool can be provided to organizations so they can look internally and preempt threat situations?</p> <p>How can you manage insider threats in all levels of government? There is no one size fits all approach.</p> <p>What is the threat? Where is it moving?</p> <p>What's needed today for leadership? How do you build it in a new manager and give them confidence, so it's done successfully? (Management Leadership system? What is a good balance of authority and empathy in management? How can we better train supervisors to interact with employees and in doing so better, decreasing insider threats?)</p>
<hr/>	
dark triad	<p>What's the algorithm for monitoring the workplace environment that identifies people with dark triad elements or those mentally disturbed/emotionally challenged?</p>
disinformation	<p>How does belief, polarization and disinformation contribute to future insider threats? Ways to combat disinformation?</p>
effective	<p>What are the positive aspects of insider risk programs? Look at taking a balanced, positive approach because too often programs are used as a hammer and people have become wary of them. These programs are not well-perceived by the public or well absorbed by the workforce. Finally, will focusing on positive aspects make programs more effective?</p>

effective	How can we mitigate insider threat without infringing upon individual rights while fulfilling organizational priorities?
indicator	What is the shelf life for an indicator?
integrity	The role of integrity. How can it be assessed? Is it a fixed trait or situationally dependent? Are there ways to increase integrity in people? Can you have greater integrity in work life vs personal life?
leaders	How do you build a culture where leaders pay attention to behavioral characteristics that could be disruptive down the road?
loyalty/culture	<p>How does incorporation of bundles influence things like loyalty and culture of organization in a measurable way? How does disinterested perceived organizational support factor in? Why is it that people trust the organization when the organization benefits employees in a way that doesn't directly benefit the organization?</p> <p>Motivational focus: Can you measure the composition of a team by an individual's motivational focus to develop a strategy that works for each particular team? How can you develop a strategy effectively based on motivational focus? (e.g., prevention focus = security? or achievement focus = promotions?)</p>
meaningful work	What should one expect to get out of work? (What makes an employee satisfied or have positive well-being)
model	<p>Lack of theoretical models for decision making we can draw from other fields (game theory, I/O literature, leadership, communications, risk-based decision making).</p> <p>Evaluate existing theoretical models and foundational concepts and packages for InT discipline.</p> <p>What is the organizational ecosystem of insider risk emergence? It's Depth and Validity? What are the variables, the mathematical model of which is more important; AI problem AI solution?</p> <p>Why do people do or not do bad things as they relate to insider threat actions? Note: social network theory of grievance distribution is important</p>

Problem: threat model (0 tolerance) draws assessments from failure case studies, very anecdotal and rare.

Dream: Why not collect detailed data on a large/diverse cohort of cleared employees on a rolling basis then analyses after 10 years

resilience How do you build trust and resilience in organizations, and preempt that threat through day-to-day observations?

How has growing up with technological advances impacted individual resilience and what are the side effects? What is the impact of technological advances on resilience? What positive coping mechanisms are available when you now face a challenge?

social justice Social justice: How do people's sense of social justice instigate them to engage InT behaviors?

What is some psychological online screening for general onboarding, especially for managers? (e.g., reliable online psychological test/screening, looking for preposition data)

How to get base predisposition data that makes managers more aware of applicants with higher InT potential?

How do we get this data? How do we develop this assessment? Have we achieved balance between empowerment of the workforce and agreeing to risk mitigation measures?

trust We need to hear from the people who we want to trust the organization; what is the "average joe employee" perspective on insider trust/threat/constructs? Also, talk to people who aren't enmeshed in the government

How to encourage people to come forward before a situation escalates?

How do you demonstrate trust to people? How to show value even when it doesn't directly benefit me?

validate How do you validate the bundling of positive and deterrence practices?

value How to value culture and individuals within organizations

wellness What are the important measures for understanding balance between workforce wellness and accountability? When organizational culture gets in the way of achieving this, how can you move it towards balance?

Conclusion

The goals of this research were to 1) identify common themes and questions among insider threat operators, researchers, and policymakers, 2) develop, refine, and expand the conceptual model of relevant constructs, and 3) develop future operationally focused research questions related to the larger program of research on insider risk/threat at ARLIS.

We noted four major recurring themes across the majority of our work.

1. *The importance of trust.* The need for solid foundational research on the relevance of trust to reducing insider risk, how to best assess trust, how best to increase trust, and the importance of trust as a part of leadership and workplace relationships were all raised as key questions for future research.
2. *The importance of good leadership and good relationships with colleagues.* The importance of cultivating and maintaining strong, healthy, and supportive relationships between colleagues, between immediate supervisors and supervisees, and between organizational leadership and employees was repeatedly highlighted. However, the greatest emphasis was given to the importance of good leadership at every level throughout an entire organization.
3. *De-emphasis on tracking individual characteristics, and the need for greater emphasis on organizational characteristics.* Individual factors (e.g., personality, individual motivation, burnout) which currently receive great attention, were largely de-emphasized in favor of greater focus on organizational level factors such as leadership and the perceptions of organizational policies (including insider threat programs).
4. *Recognition of the difficulty in, but ultimate importance of, getting ahead of threats before they manifest.* The security challenges, and opportunities, of insider risk/threat and personnel vetting are problems of the human domain, requiring successfully integrating the social and behavioral sciences in concert with technical solutions to better measure and model (characterize, quantify, predict) and mitigate (shape, exploit, prevent) emergent insider risks/threats. Gaining and maintaining advantage in human domains requires proactive, rather than reactive, interventions. By recognizing and operationalizing new predictors and indicators of increased risk, the security community will be able to build a resilient and trusted workforce – one that is much less likely to produce detrimental surprise.

The fourth key theme our SMEs identified is that gaining and maintaining advantage in human domains requires proactive, rather than reactive, interventions. The applied research questions identified in this work represent one approach to proactive work - identifying key questions in a research portfolio on addressing insider risk/threat and creating Insider TRUST. What might we stand to gain from trying to understand “what goes right” in high performing organizations where

things like building and maintaining trust among an organization and its personnel are also prioritized?

ACKNOWLEDGEMENTS

This report was prepared for [Office of the Undersecretary of Defense for Intelligence and Security (OUSD(I&S)), United States Department of Defense (DoD)] under the following agreement:

HQ003420F0655, *University of Maryland*, “Insider Threat and Personnel Vetting.”

DISCLAIMERS

Any views, opinions, findings, conclusions, or recommendations expressed in this publication do not necessarily reflect the views of an official United States government position, policy, or decision. Additionally, neither the United States government nor any of its employees make any warranty, expressed or implied, nor assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process included in this publication.

Certain commercial entities, equipment, or materials may be identified in this document to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the Applied Research Laboratory for Intelligence and Security (ARLIS), the University of Maryland, or the United States government, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

ABOUT ARLIS

Applied Research Laboratory for Intelligence and Security (ARLIS) is a UARC based at the University of Maryland College Park and established in 2018 under the auspices of the OUSD(I&S). ARLIS is intended as a long-term strategic asset for research and development in artificial intelligence, information engineering, acquisition security, and social systems. One of only 14 designated United States Department of Defense (DoD) UARCs in the nation, ARLIS conducts both classified and unclassified research spanning from basic to applied system development and works to serve the U.S. Government as an independent and objective trusted agent.

Technical Points of Contact:

PI: Adam Russell, D.Phil.

Chief Scientist, ARLIS

301.226.8834; arussell@arlis.umd.edu

Co-PI/Task Lead: Kelly Jones, Ph.D.

Assistant Research Scientist, ARLIS

301.226.8850; kjones@arlis.umd.edu

Administrative Points of Contact:

Ms. Monique Anderson

Contract Officer, Office of Research Administration

Assistant Director, ARLIS

301.405.6272; manders1@umd.edu

REFERENCES

- Alloy, L. B., Peterson, C., Abramson, L. Y., & Seligman, M. E. P. (1984). Attributional style and generality of learned helplessness. *Journal of Personality and Social Psychology*, 46(3), 681-687.
- Argenti, P. A. (2017). Strategic communication in the c-suite. *International Journal of Business Communication*, 54(2), 146-160.
- Ashton, M. C. & Lee, K. (2008). The HEXACO model of personality structure and the importance of the H factor. *Social and Personality Psychology Compass*, 2(5), 1952-1962.
- Avolio, B. J. (2007). Promoting more integrative strategies for leadership theory-building. *American Psychologist*, 62(1), 25-33.
- Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psychologist*, 37(2), 122-147.
- Bass, B. M. (1997). Does the transactional-transformational leadership paradigm transcend organizational and national boundaries? *American Psychologist*, 52(2), 130-139.
- Basu, S., Chua, Y. H. V., Lee, M. W., Lim, W. G., Maszczyk, T., Guo, Y., & Dauwels, J. (2018). Towards a data-driven behavioral approach to prediction of insider-threat. *2018 IEEE International Conference on Big Data (Big Data)*, 4994-5001.
- Carver, C. S., Scheier, M. F., & Segerstrom, S. C. (2010). Optimism. *Clinical Psychology Review*, 30(7), 879-889.
- Chemers, M. M. (1991). *An integrated theory of leadership*. Psychology Press.
- Chemers, M. M. (2000). Leadership research and theory: A functional integration. *Group Dynamics: Theory, Research, and Practice*, 4(1), 27-43.

- Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, trustworthiness, and trust propensity: A meta-analytic test of their unique relationships with risk taking and job performance. *Journal of Applied Psychology, 92*(4), 909-927.
- Costa, A. C., Fulmer, C. A., & Anderson, N. R. (2017). Trust in work teams: An integrative review, multilevel model, and future directions. *Journal of Organizational Behavior, 39*, 169-184.
- Crano, W. D. (2000). "Milestones in the psychological analysis of social influence." *Group Dynamics: Theory, Research, and Practice, 4*: 68-80. doi:10.1037/1089-2699.4.1.68.
- Dalal, R. S. (2005). A meta-analysis of the relationship between organizational citizenship behavior and counterproductive work behavior. *Journal of applied psychology, 90*(6), 1241-1255.
- Dirks, K. T. & Ferrin, D. L. (2002). Trust in leadership: Meta-analytic findings and implications for research and practice. *Journal of Applied Psychology, 87*(4), 611-628.
- Edwards, J. R. & Cable, D. M. (2009). The value of value congruence. *Journal of Applied Psychology, 94*(3), 654-677.
- Eva, N., Cox, J. W., Tse, H. H. M., Lowe, K. B. (2019). From competency to conversation: A multi-perspective approach to collective leadership development. *The Leadership Quarterly*.
- Fehr, R., Fulmer, A., & Keng-Highberger, F. T. (2019). How do employees react to leaders' unethical behavior? The role of moral disengagement. *Personnel Psychology, 73*, 73-93.
- Feitosa, J., Grossman, R., Kramer, W. S., & Salas, E. (2020). Measuring team trust: A critical and meta-analytical review. *Journal of Organizational Behavior, 41*, 479-501.
- Fiedler, F. E. (1961). A contingency model of leadership effectiveness. *Advances in Experimental Social Psychology, 1*, 149-190.
- Fiedler, F. E. (1971). *Personality and situational determinants of leader behavior*. Report prepared for Advanced Research Projects Agency, Department of the Navy and Office of Naval Research, Department of the Navy (Report No. 71-18).

- Fleishman, E. A., Mumford, M. D., Zaccaro, S. J., Levin, K. Y., Korotkin, A. L., & Hein, M. B. (1991). Taxonomic efforts in the description of leader behavior: A synthesis and functional interpretation. *The leadership quarterly*, 2, 245-287.
- Flauto, F. J. (1999). Walking the talk: The relationship between leadership and communication competence. *The Journal of Leadership Studies*, 6(1/2), 86-97.
- Forsyth, D.R. (2009). *Group Dynamics*. New York: Wadsworth
- Forsyth, D.R. (2010). "Components of cohesion." *Group Dynamics*, 5th Edition. Wadsworth: Cengage Learning. p. 118-122.
- Fulmer, A. & Dirks, K. (2018). Multilevel trust: A theoretical and practical imperative. *Journal of Trust Research*, 8(2), 137-141.
- Fulmer, C. A. & Gelfand, M. J. (2012). At what level (and in whom) we trust: Trust across multiple organizational levels. *Journal of Management*, 38(4), 1167-1230.
- Greitzer, F. L., Kangas, L. J., Noonan, C. F., Brown, C. B., & Ferryman, T. (2013). Psychosocial modeling of insider threat risk based on behavioral, and word use analysis. *Indiana University Press*, 9(1), 106-138.
- Gruys, M. L., & Sackett, P. R. (2003). Investigating the dimensionality of counterproductive work behavior. *International Journal of Selection and Assessment*, 11, 30 – 41.
- Hacker, J., Johnson, M., Saunders, C., & Thayer, A. L. (2019). Trust in virtual teams: A multidisciplinary review and integration. *Australasian Journal of Information Systems*, 23, 1-36.
- Hogg, M. A., & Williams, K. D. (2000). From I do we: Social identity and the collective self. *Group dynamics: Theory, research, and practice*, 4(1), 81.
- Kaufman, S. B., Yaden, D. B., Hyde, E., & Tsukayama, E. (2019). The light vs. dark triad of personality: Contrasting two very different profiles of human nature. *Frontiers in Psychology*, 10, 467.

- Kilburg, R. R. & Donohue, M. D. (2011). Toward a “grand unifying theory” of leadership: Implications for consulting psychology. *Consulting Psychology Journal: Practice and Research*, 63(1), 6-25.
- Kirkpatrick, S. A. & Locke, E. A. (1996). Direct and indirect effects of three core charismatic leadership components on performance and attitudes. *Journal of Applied Psychology*, 81(1), 36-51.
- Kish-Gephart, J. J., Harrison, D. A., & Treviño, L. K. (2010). Bad apples, bad cases, and bad barrels: meta-analytic evidence about sources of unethical decisions at work. *Journal of applied psychology*, 95(1), 1-31.
- Koçyiğit, Y. and Akkaya, B., 2020. The role of organizational flexibility in organizational agility: A research on SMEs. *Business Management and Strategy*, 11, pp.110-123.
- Larson, G. S. & Pepper, G. L. (2003). Strategies for managing multiple organizational identifications: A case of competing identities. *Management Communication Quarterly*, 16(4), 528-557.
- Lewicki, R. J., Tomlinson, E. C., & Gillespie, N. (2006). Models of interpersonal trust development: Theoretical approaches, empirical evidence, and future directions. *Journal of Management*, 32(6), 991-1022.
- Longenecker, C., & Insch, G. S. (2018). Senior leaders’ strategic role in leadership development. *Strategic HR Review*.
- Marks, M. A., Mathieu, J. E., & Zaccaro, S. J. (2001). A temporally based framework and taxonomy of team processes. *Academy of management review*, 26, 356-376.
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3), 709-734.
- McCrae, R. R. & Costa, P. T. (1987). Validation of the five-factor model of personality across instruments and observers. *Journal of Personality and Social Psychology*, 52(1), 81-90.

- Mumford, M. D., Scott, G. M., Gaddis, B., & Strange, J. M. (2002). Leading creative people: Orchestrating expertise and relationships. *The Leadership Quarterly, 13*, 705-750.
- O'Keefe, D. J. (2002). *Persuasion: Theory and research* (2nd ed.). Thousand Oaks, CA: Sage.
- Organ, D. W. (1997). Organizational citizenships behavior: It's construct cleanup time. *Human Performance, 10*, 85-97.
- Paul, H., Garg, P. (2012). Mutualistic perspective of individual resilience and organizational commitment: A path analysis model. *International Journal of Management and Behavioural Sciences, 1*, 107-119.
- Paulhus, D. L. & Williams, K. M. (2002). The dark triad of personality: Narcissism, machiavellianism, and psychopathy. *Journal of Research in Personality, 36*(6), 556-563.
- Peterson, C., & Steen, T. (2009). Optimistic explanatory style. In S.J. Lopez & C.R. Snyder (eds.) *The Oxford handbook of positive psychology* (pp. 313-322). Oxford University Press.
- Podsakoff, N. P., Whiting, S. W., Podsakoff, P. M., & Blume, B. D. (2009). Individual-and organizational-level consequences of organizational citizenship behaviors: A meta-analysis. *Journal of applied Psychology, 94*(1), 122-141.
- Popper, M., Mayseless, O., & Castelnovo, O. (2000). Transformational leadership and attachment. *Leadership Quarterly, 11*(2), 267-289.
- Postmes, T., Tanis, M., & de Wit, B. (2001). Communication and commitment in organizations: A social identity approach. *Group Processes & Intergroup Relations, 4*(3), 227-246.
- Powers, E. L. (2000). Employee loyalty in the new millennium. *SAM Advanced Management Journal, 65*(3), 4.
- Rotter, J. B. (1966). Generalized expectancies for internal versus external control of reinforcement. *Psychological Monographs: General and Applied, 80*(1), 1-28.

- Ryan, R. M., & Deci, E. L. (2001). On happiness and human potentials: A review of research on hedonic and eudemonic wellbeing. *Annual Review Psychology*, 52(1), 141–166.
- Sama, L. M., & Shoaf, V. (2008). Ethical leadership for the professions: Fostering a moral community. *Journal of Business Ethics*, 78, 39-46.
- Sargent, L. D. & Waters, L. E. (2004). Careers and academic research collaborations: An inductive process framework for understanding successful collaborations. *Journal of Vocational Behavior*, 64, 308-319.
- Schnackenberg, A. K., & Tomlinson, E. C. (2016). Organizational transparency: a new perspective on managing trust in organization-stakeholder relationships. *Journal of Management*, 42(7), 1784–1810. <https://doi.org/10.1177/0149206314525202>
- Sipe, L. J. (2018). Leadership, innovation outputs, and business performance: a mixed methods study of senior managers in the attractions industry. *International Journal of Hospitality & Tourism Administration*, 19(4), 440-463.
- Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of management review*, 20(3), 571-610.
- Tomlinson, E. C., Schnackenberg, A. K., Dawley, D., & Ash, S. R. (2018). Revisiting the trustworthiness-trust relationship: Exploring the differential predictors of cognition- and affect-based trust. *Journal of Organizational Behavior*, 41, 535-550.
- Tosi, H. L., Misangyi, V. F., Fanelli, A., Waldman, D. A., & Yammarino, F. J. (2004). CEO charisma, compensation, and firm performance. *The Leadership Quarterly*, 15, 405-420.
- Wang, D. S., & Hsieh, C. C. (2013). The effect of authentic leadership on employee trust and employee engagement. *Social Behavior and Personality: an international journal*, 41, 613-624.

Williams, M. (2001). In whom we trust: Group membership as an affective context for trust development. *The Academy of Management Review*, 26, 377-396.

Worden, S. (2003). The role of integrity as a mediator in strategic leadership: a recipe for reputational capital. *Journal of Business Ethics*, 46(1), 31-44.

Yukl, G. & Mahsud, R. (2010). Why flexible and adaptive leadership is essential. *Consulting Psychology Journal: Practice and Research*, 62(2), 81-93.

Appendix 1: Applied Research Questions

Complied list of all applied research questions from SMEs and literature review.

General questions:

1. What theoretical models for decision making can be leveraged or built for insider risk and Insider TRUST? How can we effectively draw research from other fields (e.g., game theory, Industrial/Organizational psychology, management, communications, risk-based decision making), making sure that what we draw is relevant and applicable for insider risk/threat contexts (both the theoretical model and its foundational concepts)?
2. What is the effect of the information environment on insider risk/threats and Insider TRUST? Do belief polarization and disinformation contribute to increased risk of insider events? If they do, what are the best techniques for decreasing risks of inside events that are influenced by disinformation?
3. What is the larger organizational ecosystem from which insider risks emerge? What is the best way to model that ecosystem?
4. How do we link research, and operational best practices, that addresses the immutably sociotechnical nature of the human domain challenges we face across the entire interdependent supply chain of products, services, workforces, and workplaces?

Trust:

1. Applied research question: what is the effect of increasing different trustworthiness indicators among leaders for creating successful workplace environments?
2. What are the effects of asymmetrical trust, where one party has a higher level of trust than the other?
3. What are the effects of shifting organizational and team boundaries, such as working with or across multiple teams or projects?
4. What are the effects of time or sudden environmental changes to trust across levels of relationships?
5. The migration of many to virtual or hybrid work environments also presents unique questions regarding the development and maintenance of trust across individual, team, and organizational levels when the traditional face-to-face interactions that form the basis of most relationships take place over electronic mediums (Hacker, Saunders, & Thayer, 2019).
6. How do we [organizations, leadership, or insider threat programs] demonstrate to employees that they are valued and trusted by their organization? How do we provide them with avenues to receive assistance when needed and/or to build resilience, skills, and capabilities?
6. How do we take into account trustworthiness variables in our calculations of risk? How do we build systems that consider trustworthiness (and training, resilience, and other social behavioral factors) in risk assessments?
7. How do insider threat programs [and leaders/organizations] consistently demonstrate to employees that they [the programs/leaders/organizations] are worthy of trust? Specifically, how can programs [leaders/organizations] demonstrate the four components of

trustworthiness, ability, benevolence, behavioral integrity, and values congruence? What impact does demonstrating trustworthiness have on decreasing risk and increasing desired behaviors (such as compliance with security policies, reporting concerns)? What aspects of trustworthiness in leaders are most important to decreasing insider risk?

- a. This was repeatedly mentioned by several SMEs, who all stressed that trust is a two-way street and must be earned on both sides – leaders and employees – though most of their focus was on leadership’s actions and need to demonstrate trustworthiness and to be deserving of trust from their subordinates (see Leadership section below).
8. How do we best identify trustworthy leaders, then train them to best demonstrate trust in their supervisees? For example, training in demonstrating empathy was mentioned by several SMEs.
9. What is the perspective of those whom we ask to trust in insider threat programs, leadership, and the organization (the ‘average joe’ employee)?
 - a. An SME rightly pointed out that much of the research on insider threat, including the current effort, focuses more on eliciting input from those already in managerial or policy positions, who likely have greater insight into the functions of insider threat programs and organizations as a whole, and that research could benefit from greater insights from those who are outside those groups.
10. How do insider threat programs, leaders, and organizations, best build and communicate shared visions of addressing insider risk and building Insider TRUST? How effective are such messages in decreasing risk? Who are the best messengers of shared visions – leaders?
11. Is an effective way to build Insider TRUST through identifying and training leaders (and future leaders) in best leadership practices (e.g., demonstrating respect and valuing employees, setting, and living up to organizational standards and expectations, clear communication)?

Leadership

1. Applied research question (SME suggested): How do we best identify good (potential) leaders? What training should they be provided?
 - a. SMEs repeatedly stressed the importance of training for leaders, including both training in insider risk mitigation (identification of concerning behaviors, intervention techniques, reporting requirements), but also in best leadership practices including empathy/concern, integrity, fairness, and competence.
 - b. Empirical literature supports the idea that early and continuous training for leaders is linked to increased organizational success (Longenecker & Insch, 2018), what is currently unknown is the effectiveness in decreasing insider risks/threats or increasing Insider TRUST.
2. Applied research question: how do insider threat programs, leaders, and organizations, best build and communicate shared visions of addressing insider risk and building Insider TRUST? How effective are such messages in decreasing risk? Who are the best messengers of shared visions – leaders?

3. Directly linking trust/trustworthiness and leadership constructs in this review, trust in leadership by subordinates has been linked to positive attitudes, behaviors, and performance outcomes in the workplace (Dirks & Ferrin, 2002). Is an effective way to build Insider TRUST through identifying and training leaders (and future leaders) in best leadership practices (e.g., demonstrating respect and valuing employees, setting and living up to organizational standards and expectations, clear communication)?
 - a. Several SMEs asserted that trust in leadership is related to loyalty to organizations and buy-in to organizational mission.
4. Changing and complex environments means that leadership requirements will change (see recent shift to *collective leadership research*, where leadership is studied as it is distributed across multiple members within an organization, e.g., Eva, Cox, Tse, & Lowe, 2019). What elements of best leadership practices will remain constant over time and what will need to change in order to retain our advantage in the human domain?
5. What elements of best leadership practices will remain constant over time and what will need to change in order to retain our advantage in the human domain?

Subconstructs relating trust & leadership (integrity, Credibility, and Legitimacy, loyalty, & transparency)

1. consistently demonstrating integrity, credibility, and legitimacy is the best way to earn trust; while failing to live up to these standards is the fastest way to break trust.
2. Applied research question from SME: Can integrity be assessed effectively? If so, how can it be best incorporated in judgements of risk or trust?
3. What kinds of loyalty (to different referents) are most important to building Insider TRUST?
4. While trust is a key factor in creating loyalty, what other factors (e.g., organizational supportiveness) create loyalty?
5. what effect does greater transparency regarding the process of counter insider threat programs have on perceptions of the programs?

Wellbeing & Resilience

1. Applied research question from SME: what are the effects of respect and empathy on risks of different types of insider threat events?
2. Applied research question: what is the role of wellbeing in mitigating risks of insider events? What is its role in building Insider TRUST?
3. Applied research question from SME: how can we build trust and resilience throughout organizations to mitigate risk?
4. Applied research question from SME: are there impacts of technological advances on building resilience?
5. Applied research question from SME: does leadership making resilience a priority for their organizations decrease risks of insider events? Can leadership contribute to building individual employee's resilience? Does individual resilience contribute to organizational resilience (and can that impact be measured)?

6. Applied research question from SME: can good leaders impact resilience by calibrating expectations of employees and team (in other words, by not overloading them with more than they can handle)?

Additional Questions Identified by SMEs during Interviews

balance	How do you balance individual and organizational concerns?
behavior	<p>What is the empirical connectivity between workplace and external factors on ultimate behavioral outcomes?</p> <p>How do you address those potentially problematic/disruptive behavioral characteristics?</p>
bystanders	What is the role of bystanders and bystanders of bystanders in reporting InT?
case studies	Do in depth case studies of organizations that created conditions/policies that we and others believe led to lower levels of risk; and organizations that led to higher risk; ask interdisciplinary group to go through that and see what they thought was critical.
CInT	<p>What tool can be provided to organizations so they can look internally and preempt threat situations?</p> <p>How can you manage insider threats in all levels of government? There is no one size fits all approach.</p> <p>What is the threat? Where is it moving?</p> <p>What’s needed today for leadership? How do you build it in a new manager and give them confidence, so it’s done successfully? (Management Leadership system? What is a good balance of authority and empathy in management? How can we better train supervisors to interact with employees and in doing so better, decreasing insider threats?)</p>
dark triad	What's the algorithm for monitoring the workplace environment that identifies people with dark triad elements or those mentally disturbed/emotionally challenged?
disinformation	How does belief, polarization and disinformation contribute to future insider threats? Ways to combat disinformation?

effective	What are the positive aspects of insider risk programs? Look at taking a balanced, positive approach because too often programs are used as a hammer and people have become wary of them. These programs are not well-perceived by the public or well absorbed by the workforce. Finally, will focusing on positive aspects make programs more effective?
effective	How can we mitigate insider threat without infringing upon individual rights while fulfilling organizational priorities?
indicator	What is the shelf life for an indicator?
integrity	The role of integrity. How can it be assessed? Is it a fixed trait or situationally dependent? Are there ways to increase integrity in people? Can you have greater integrity in work life vs personal life?
leaders	How do you build a culture where leaders pay attention to behavioral characteristics that could be disruptive down the road?
loyalty/culture	How does incorporation of bundles influence things like loyalty and culture of organization in a measurable way? How does disinterested perceived organizational support factor in? Why is it that people trust the organization when the organization benefits employees in a way that doesn't directly benefit the organization? Motivational focus: Can you measure the composition of a team by an individual's motivational focus to develop a strategy that works for each particular team? How can you develop a strategy effectively based on motivational focus? (e.g., prevention focus = security? or achievement focus = promotions?)
meaningful work	What should one expect to get out of work? (What makes an employee satisfied or have positive well-being)
model	Lack of theoretical models for decision making we can draw from other fields (game theory, I/O literature, leadership, communications, risk-based decision making). Evaluate existing theoretical models and foundational concepts and packages for InT discipline.

What is the organizational ecosystem of insider risk emergence? It's Depth and Validity? What are the variables, the mathematical model of which is more important; AI problem AI solution?

Why do people do or not do bad things as they relate to insider threat actions?
Note: social network theory of grievance distribution is important

Problem: threat model (0 tolerance) draws assessments from failure case studies, very anecdotal and rare.

Dream: Why not collect detailed data on a large/diverse cohort of cleared employees on a rolling basis then analyses after 10 years

resilience

How do you build trust and resilience in organizations, and preempt that threat through day-to-day observations?

How has growing up with technological advances impacted individual resilience and what are the side effects? What is the impact of technological advances on resilience? What positive coping mechanisms are available when you now face a challenge?

social justice

Social justice: How do people's sense of social justice instigate them to engage InT behaviors?

What is some psychological online screening for general onboarding, especially for managers? (e.g., reliable online psychological test/screening, looking for preposition data?

How to get base predisposition data that makes managers more aware of applicants with higher InT potential?

How do we get this data? How do we develop this assessment? Have we achieved balance between empowerment of the workforce and agreeing to risk mitigation measures?

trust

We need to hear from the people who we want to trust the organization; what is the "average joe employee" perspective on insider trust/threat/constructs? Also, talk to people who aren't enmeshed in the government

How to encourage people to come forward before a situation escalates?

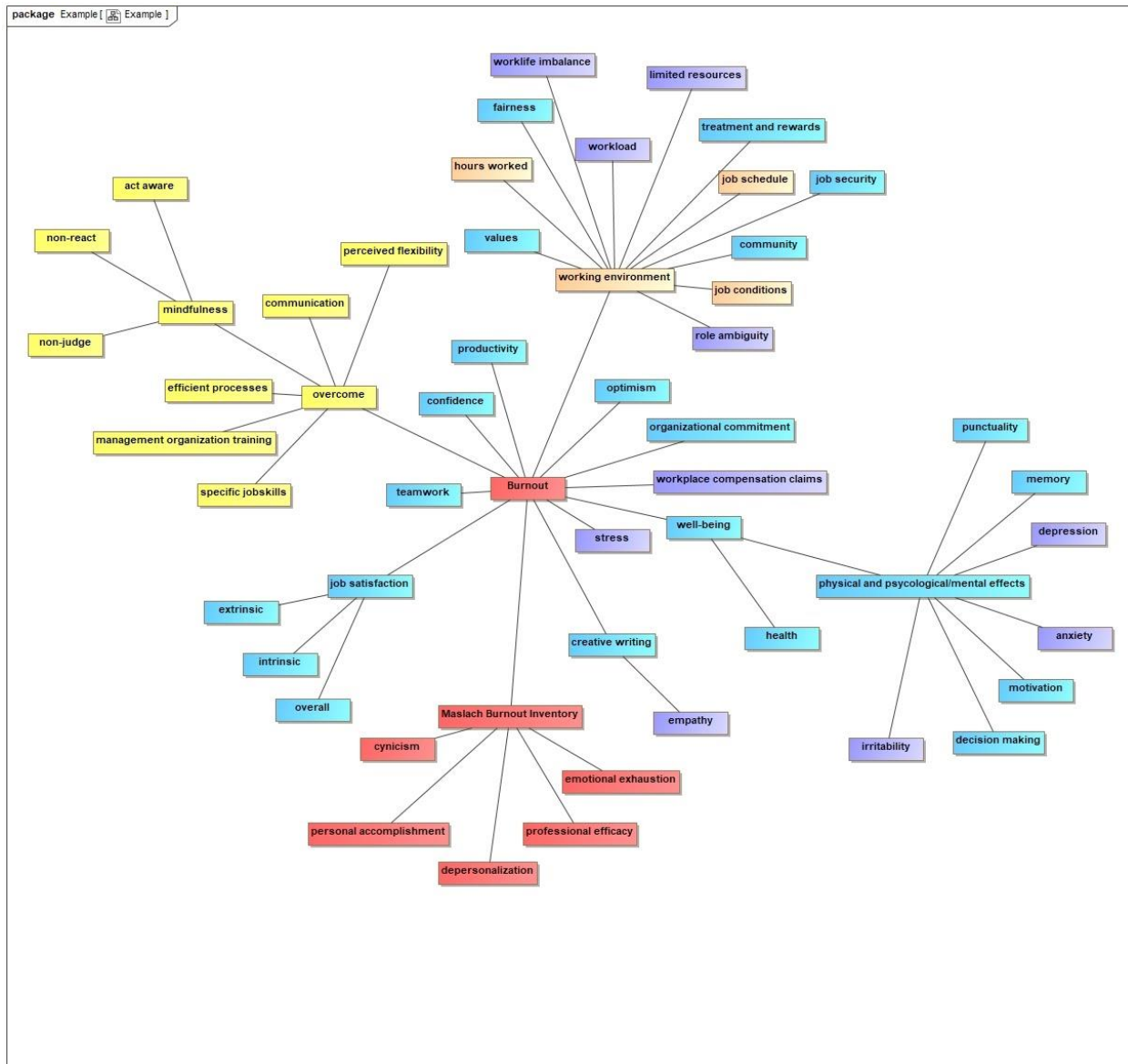
How do you demonstrate trust to people? How to show value even when it doesn't directly benefit me?

- validate How do you validate the bundling of positive and deterrence practices?
- value How to value culture and individuals within organizations?
- wellness What are the important measures for understanding balance between workforce wellness and accountability? When organizational culture gets in the way of achieving this, how can you move it towards balance?

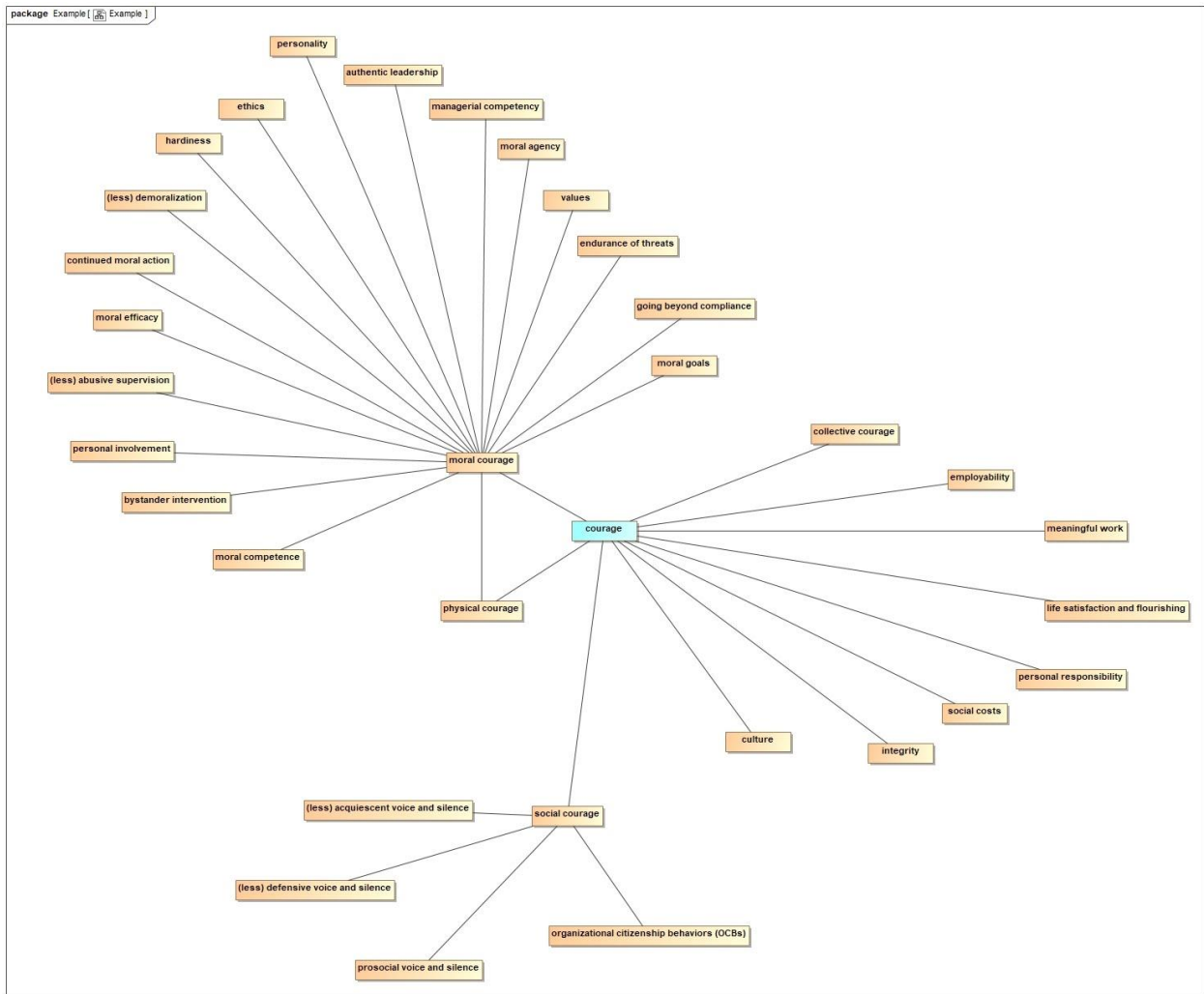
APPENDIX 2: Construct Maps

The following factors were all explored as part of our literature review on Insider TRUST. However, in soliciting input from SMEs, they ranked these constructs as ‘somewhat’ or ‘least important’ and had few to no suggestions for applications or future research questions. The majority of these factors center on the fixed or trait characteristics of individual (rather than the organization). We include the construct maps we developed based on the literature for future reference on the following factors (in alphabetical order): Burnout, Courage, Incentives, Malevolent creativity, Meaningful work, Motivation, Optimism, Personality.

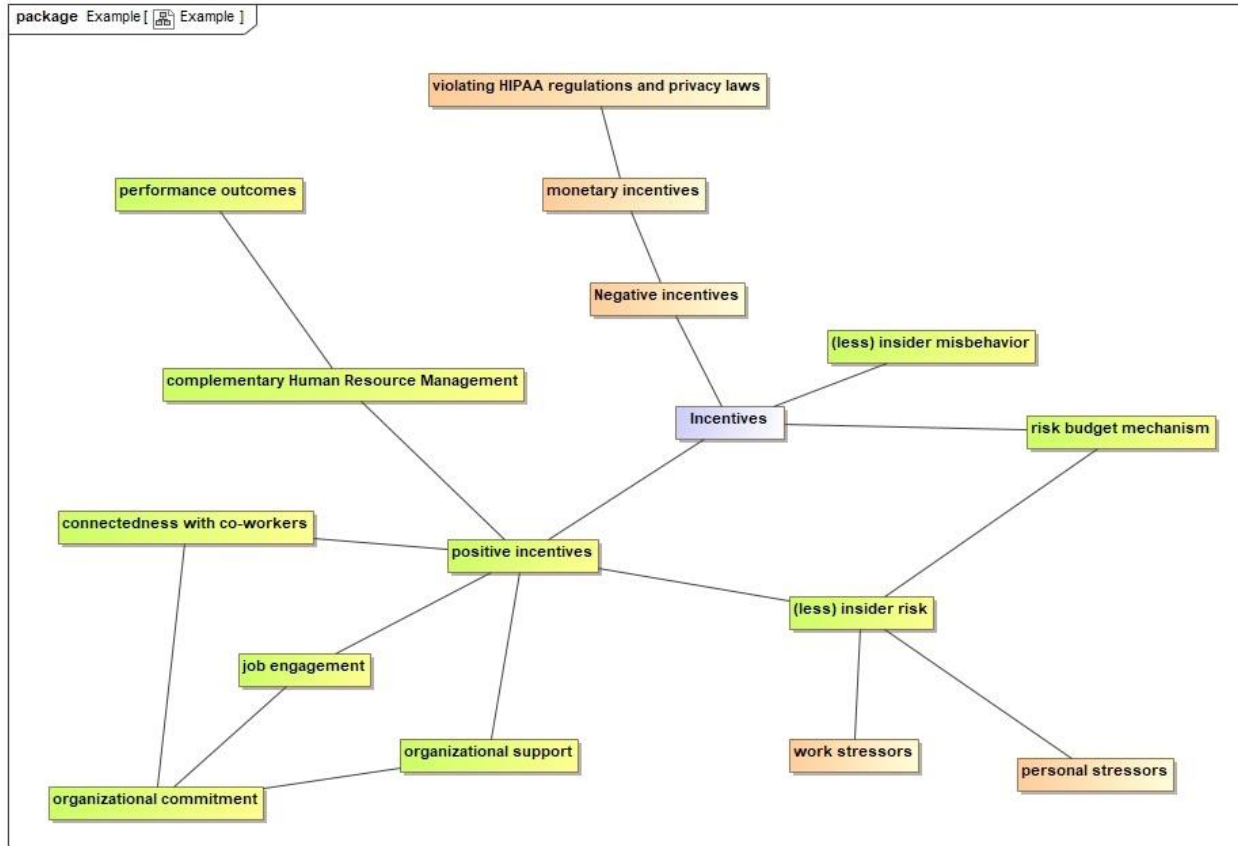
Burnout Construct Map – relationships to other constructs identified in the literature



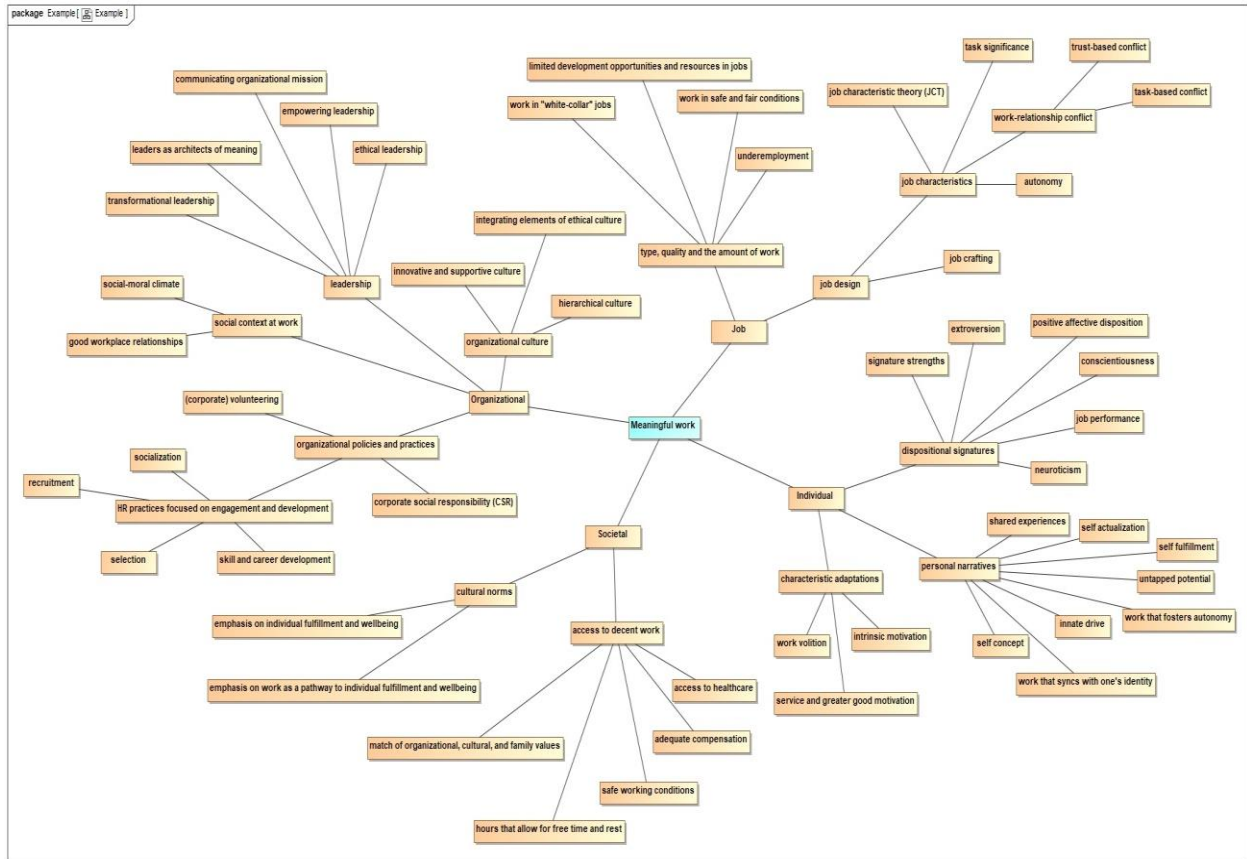
Courage Construct Map - relationships to other constructs identified in the literature



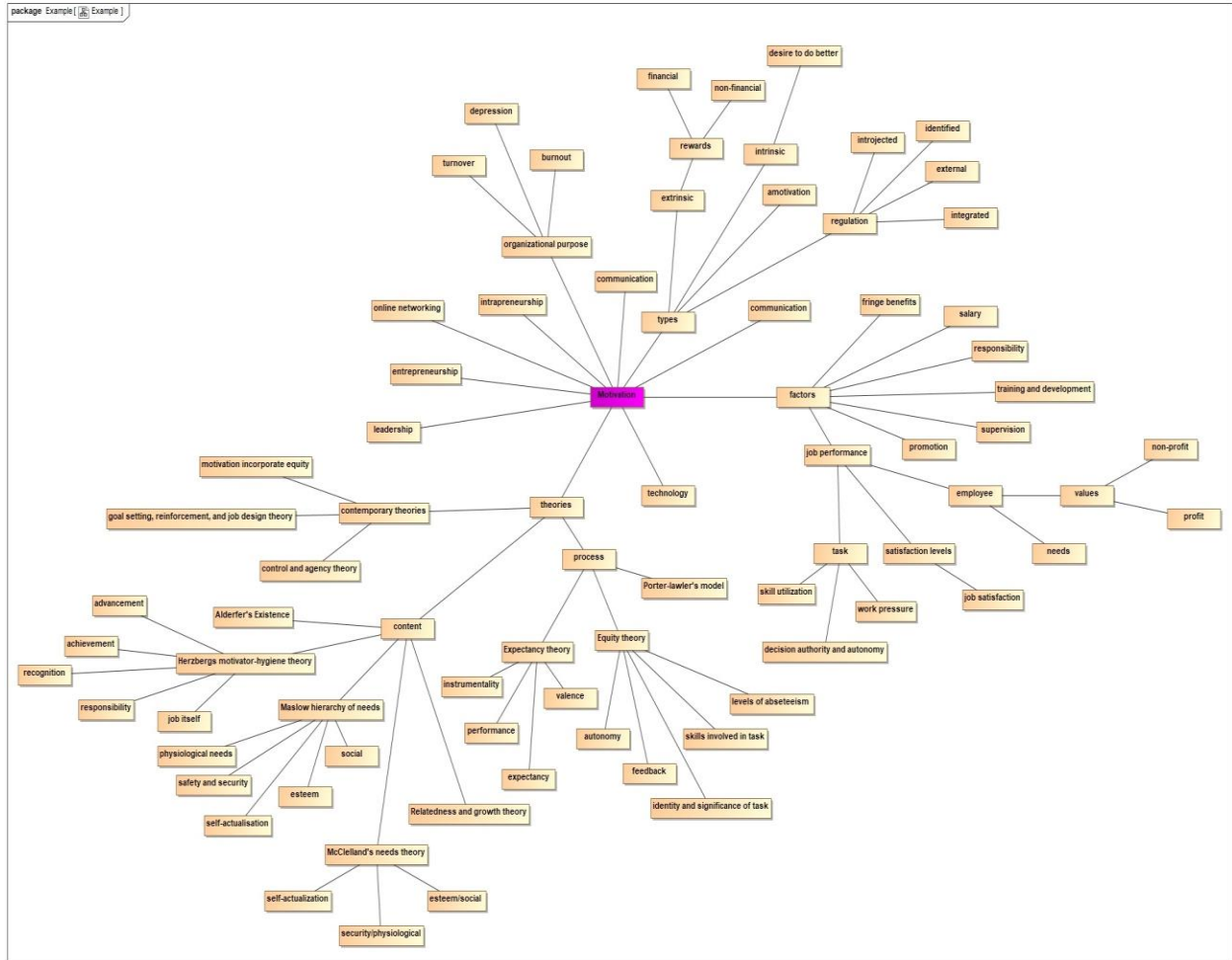
Incentives Construct Map - relationships to other constructs identified in the literature



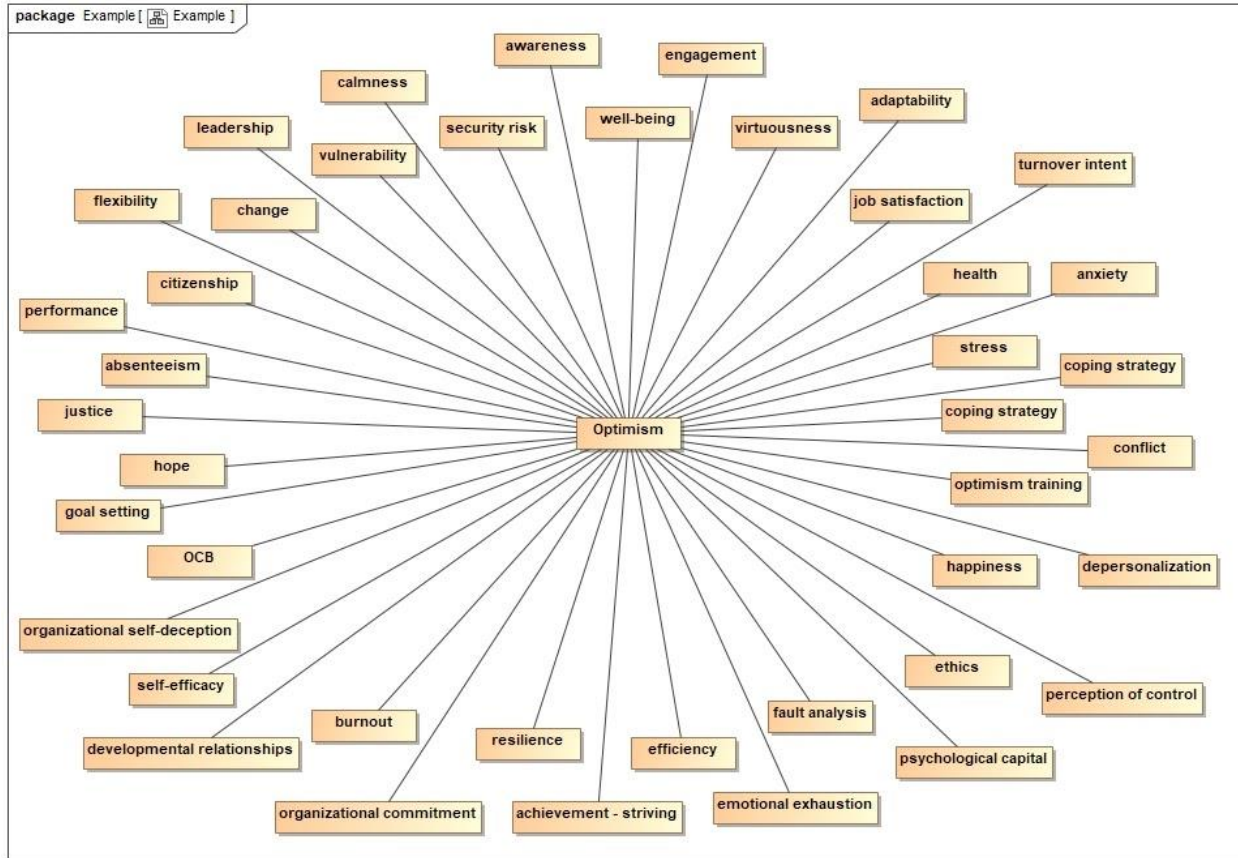
Meaningful work Construct Map – relationships to other constructs identified in the literature



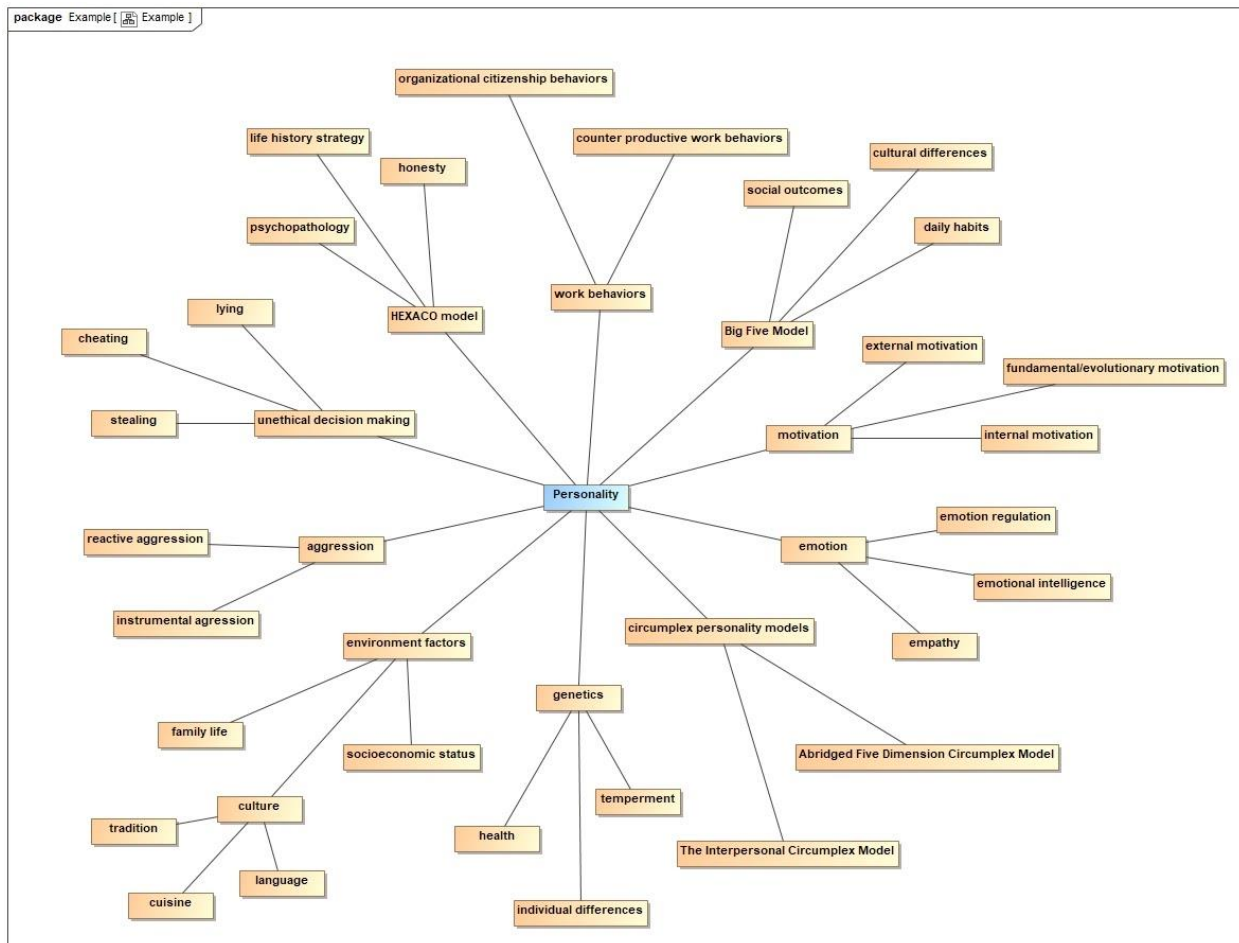
Motivation Construct Map - relationships to other constructs identified in the literature



Optimism Construct Map - relationships to other constructs identified in the literature



Personality Construct Map - relationships to other constructs identified in the literature



APPENDIX 3: Subject Matter Expert Interview Materials

Semi-structured interview protocol

Date & time: __date__, __time__

Interviewee: __name__

Greetings and introductions.

1 - Briefly describe the duration and nature of your current and previous professional experience working on insider threats (research, operational, policy, or other).

Estimated time: 2 minutes

2 - What Insider TRUST constructs do you consider to be among the 5 most important?

Estimated time 5 – 7 minutes

3 - Based on our current model, please sort the list of constructs into three categories: most important to Insider TRUST, somewhat important, least important. We're interested in your initial thoughts and reactions. As you sort, please tell us why you are putting each construct in the category, and your definition of the construct. Are there any constructs you think are missing?

Estimated time 15 – 20 minutes

4 - Based on your experience, what are the best (positive?) ways mitigate insider risk and/or build Insider TRUST?

Estimated time 5 – 8 minutes

5 - Based on our conversation today and what you've seen about Insider TRUST, what are the most important questions that you think should be the first focus of future research? What are the questions about mitigating risks of insider events that you do not currently have answers to?

Estimated time: 5 – 10 minutes

Thank you for taking the time to talk with us today. We really appreciate it! Now that we've had this conversation and shared ideas, we'd appreciate if you would take a few minutes and look back over the construct maps we provided and see if anything strikes you. We're especially interested in anything you think might be missing from the maps (concepts or relationships), things you think should be removed or added, additional related questions we should explore, or further questions you have.

Wrap up and thank you.

Total time: 1 hour

Question 3 Materials for Construct Sort

SMEs were presented with either Construct List A or Construct List B using a tool in Google suite called JamBoard. The interviewer screen shared (all interviews were conducted via Zoom). SMEs talked through each construct, first placing in a category, then explaining why. The interviewer moved the appropriate card into each category as the SME spoke.

Version A

Burnout	Incentives	Most Important	Somewhat Important	Least Important
Trust	Motivation			
Dark Triad	Transparency			
Empathy	Resilience			
Legitimacy	Integrity			
Creativity	OB-Counterproductive Workplace (CWB)			
Other Constructs				

Version B

CSuite (CEOs and Senior Leadership)	Organizational Citizenship Behavior (OCB)	Most Important	Somewhat Important	Least Important
Loyalty	The Light Triad			
Well-Being	Group/Team Dynamics			
Meaningful Work	Credibility			
Optimism	Personality			
Courage	Individual Differences			
Malevolent Creativity		Other Constructs		

Construct Definitions

SMEs occasionally asked for definitions of constructs or terms, which were read by the interviewer from this list. Note that these are conversational definitions.

Group A

1. Burnout: A type of psychological stress or syndrome characterized by emotional depletion, loss of motivation, reduced commitment, and exhaustion (emotional, physical). Results in reduced efficacy and increased mental distance from job or feelings of negativity towards job.
2. Citizenship: The nature/quality of an individual's response to membership in a community
3. Creativity: The ability to generate or recognize ideas or alternatives that may be useful for problem solving, communication, production of work, etc.
4. Dark Triad: Three components, including narcissism (grandiosity, ego-centric, lack of empathy), Machiavellianism (manipulation of others, a-morality, unemotional), and psychopathy (lack of remorse, callous/unemotional, antisocial behavior, impulsive).
 - a. *Note: antisocial behavior refers to that which violates the basic rights of others/harms or has no consideration for others. Antisocial behavior does NOT mean shy/reclusive behavior*
 - b. *Note: psychopathy/antisocial behavior is not synonymous with violent behavior, per se, but may sometimes involve physical/emotional violence towards others*
5. Empathy: The ability to understand what others are feeling, why they are feeling that way, and express compassion if they are in need.
6. Incentives: Something that motivates or encourages a behavior. Incentives can be of varying types such as economic (monetary), social (praise, acceptance), or moral (doing the right thing, helping someone).
7. Integrity: Honesty, strong moral and ethical principles, always doing the right thing, no matter if people are watching or who is watching
8. Legitimacy: Psychological property of an authority, institution, or social arrangement that leads those connected to it to believe that it is appropriate, proper, and just
9. Motivation: The process or reason(s) that initiate, guide, and maintain behavior
10. OB-Counterproductive Workplace (CWB): Behavior that undermines the interests of a workplace/organization/agency.
11. Resilience: The ability to withstand or recover from adversity/difficulties
12. Transparency: Used in the figurative sense to describe a state of operations/being that allow others to see what is happening. Often related to concepts such as openness, communication, and accountability.
13. Trust: Belief in the reliability, honesty, or ability of someone/something

Group B

1. Credibility: The quality of being perceived as a trustworthy, reliable source of information.
2. Courage: The quality of enduring challenges and danger without fear (i.e., bravery)
3. CSuite (CEOs and Senior Leadership): The executive level managers and leadership of an organization that work together to ensure a company stays true to its established plans and policies.

4. Group/Team Dynamics: The quality of relationships between the members of a group that can impact how the team functions and achieves its goals.
5. Individual Differences: The gamut of personal differences that affects how a person interacts with others and the environment, including, but not limited to, personality, culture, learning styles, emotion regulation, and physical characteristics.
6. Light Triad: There are three components: Faith in Humanity (belief that, generally speaking, humans are good; Humanism (all humans deserve respect and appreciation); Kantianism (people are intrinsically important and should not be exploited as pawns in a game)
7. Loyalty: The quality of being faithful to one's allegiances and agreements.
8. Malevolent Creativity: The ability to use creativity to achieve nefarious goals or develop harmful inventions.
9. Meaningful Work: Work that is perceived as important and allows workers to feel connected to a higher purpose (e.g., protecting one's country, helping one's community, serving one's God).
10. Optimism: To look at the world in a positive manner and believe that one has the ability to change one's life or the world for the better.
11. Organizational Citizenship Behavior (OCB): A person's voluntary commitment within an organization or company that is not part of his or her contractual tasks (i.e., going above and beyond one's obligatory duties).
12. Personality: The constellation of characteristics or traits of a human being that governs how one thinks, feels, and behaves across a variety of situations.
13. Well-Being: One's current levels of health, happiness, and prosperity.