Cyber Security Awareness Platform

Mulpuru Charishma
CSE
KL University
Vijayawada,India
mulpurucharishma@gmail.com

Ragam Ganesh Babu
CSE
KL University
Vijayawada,India
gannu0316@gmail.com

Abhinav Raj
CSE
KL University
Vijayawada,India
abhinavraj13112005@gmail.com

Under the guidance of

Dr. B Samatha
Associate Professor
CSE
KL University
Vijayawada,India
bsamatha@kluniversity.in

Abstract

While significant investments have been made to support new cyber security technologies, there is still a reliance on humans to withstand the actions of attackers or other malicious actors. Cybersecurity is fundamentally about an organization's ability to protect its assets from those who wish to do harm; therefore, cyber security has changed from simply being about technology to having a much broader mission — that of developing human resources and enabling employees to be more effective protectors of the organization's assets. This paper presents the Cognitive Resilience Framework for Cyber Security (CRFCS) as a new model of an organization's ability to protect against cyberattack, focusing on how to create psychological capital for the personnel within the organization to ensure their psychosocial resilience to cyberattack. Human security capabilities should be viewed as renewable resource based on a combination of cognitive psychology, organizational behavior theory and security science. Thus, it is imperative to reframe the concept of organization security from a compliance-driven training approach to one that facilitates building human security abilities as part of the overall organizational capabilities of building human assets. This work provides the methodology to develop, measure and leverage human security as strategic organizations capability. Keywords continue to include Psychological capital, cyber security from a human-centric approach, security self-efficacy, threat vigilance, cognitive security architecture.

Keywords—component, formatting, style, styling, insert

I. INTRODUCTION

1.1 The Continuing Human Factor Paradox

In the modern-day dialogue concerning cyber security, humans have consistently been referred to as being the "weakest link" within cyber security. This is a deficit oriented perspective, thus, humans are viewed as being a liability in the security system and need to be contained (limited) to the extent possible by layer(s) of technical controls, to offset the impacts resulting from human fallibility. Millions of dollars have been spent on technical controls (hundreds of billions each year) to compensate for the negative effects of human fallibility. Yet, despite having the latest technology, statisticians still report that occurrences of breaches occur because cyber criminals utilize human cognitive and social weaknesses successfully. Therefore, there is a disconnect

between the models of Security (Cyber Security) and human psychology.

Cyber Security models are still based on an outdated and erroneous assumption that a person can be trained or conditioned like a machine. When designing and implementing a Cyber Security model, policy and procedures and periodic training are the only two things that need to be considered. This view does not take into consideration the years of research conducted in Cognitive Psychology, which clearly indicates that Human decision making, threat perception and stable behaviors are all complex cognitive psychological phenomena that are determined by an individual's personal history, the context of the situation, the culture of the organization, and the cognitive resources available.

1.2 From Awareness to Cognitive Resilience

Security awareness programs have evolved over three decades from basic computer literacy training to sophisticated behavioral interventions yet remain bound to a reactive deficit-reduction paradigm. Most programs today seek to eradicate security-negative behaviors by providing knowledge, fear appeals, and compliance enforcement. However, human security competence is more fruitfully conceptualized as an emergent positive capability in need of development rather than a deficit in need of correction.

We propose cognitive resilience as the conceptual underpinning for next-generation human-centric security. Cognitive resilience denotes the mental resources that equip individuals to cope with cognitive load, social pressure, time constraints, and manipulative attempts while sustaining security-desired behavior. This reflects a basic paradigm shift: instead of trying to prevent bad behaviors, the focus shifts to establishing positive security capabilities.

1.3 Research Objectives and Contributions

Contributions: The main theoretical contributions of the paper can be pointed out as follows:
1)Conceptual Innovation: Introduces cognitive resilience as a unifying theoretical construct for human security competence, integrating hitherto fragmented research streams.
2)Framework Development: A holistic four-dimensional model of psychological capital is put forward with clear conceptual bounds and implications for measures.
3)Theoretical integration: an attempt to bind cognitive psychology, organizational behavior, and information security research into a single theoretical framework.
4)Paradigm Challenge: There is a theoretical underpinning that guides the shift from deficit-oriented security awareness to asset-oriented capability development.
5)Research Agenda: Identifies critical theoretical deficiencies and also outlines the direction for future research.

1.4 The structure of Paper

In Section 2, this paper will present theoretical foundations of cognition from psychology, resilience research, and organization capital theory. In Section 3, we will describe the Cognitive Resilience Framework for Cyber Security which includes the four dimensions and their relationships. The development of the Cognitive Security Resilience's antecedents, processes, and impact will be the focus of Section 4. Table 5 discusses aspects of measurement and operationalizing the Cognitive Resilience Framework for Cyber Security. Table 6 analyses the relevant aspects of how an organization can create a security culture and climate. In the last section of this paper we will highlight future areas of research and theoretical limitations of Cognitive Resilience in Cyber Security. In Section 8, we conclude with the implications for theory and practice.

II. METHODOLOGY

2.1 The Theory of Decision Making in Security, Existing Cognitive Psychology:

Most decisions regarding human security are based upon cognitive psychological behavior through cognitive processes in our daily lives. Theories that illustrate the Cognitive Psychology fundamentals in their application to Security Decision-Making would be as follows:
Dual-Process Theory refer to the distinction between 2 types of cognitive processing, which would be referred to as "Automatic Processing (System 1)" and "Deliberate Processing (System 2)." When a person has to make security-related decisions and operate within the constraints (time, distractions, routine) that apply to Automatic Processing; Cognitive Heuristics will be used with the intent of exploiting the individual by a "Social Engineer." In contrast, Cognitive Resource requirements will exist in order to provide Deliberative Processing when security conditions present themselves, which create the need for an individual to engage in deliberate cognitive processing. The theory of Dual Process Theory supports that to provide secure conditions through habitual responses through automatic processing of Security decisions through Automatic Processing; and provide opportunity for evolving Deliberate Cognitive Processing when threats exist.

Humans will make decisions based upon their cognitive capabilities; therefore, they can only make decisions based on what they know at the time of the decision. Therefore, everyone's decision will not be the same. In other words, there is a limit to what people are able to think about at the same time when they are attempting to make a decision. This is known as "**bounded rationality**". For security, this shows that if a security policy or procedure is too complicated it will eventually be made easier by whatever way it can be. Therefore, the design of security systems should take into consideration the cognitive abilities of a human.

Cognitive load theory shows how working memory limitations affect learning and performance. Security activities that have a high cognitive load (i.e., elaborate classification schemes and complex authentication processes) reduce the ability to do the primary job and increase the likelihood of errors. Therefore, when security training is performed while the employee is under a high cognitive load, it will be more difficult for the employee to retain the information learned. The key points to take away from cognitive load theory are to reduce any unnecessary cognitive loads in security processes and to maximize any beneficial cognitive loads during security training.

Signal Detection Theory (SDT) helps explain how to identify threats in a security environment. The challenge to a vigilant security career is that the rare nature of a threat is defined by an abundance of non-threats (i.e., benign events) that occur within the environment. Consequently, sustaining vigilance over an extended period of time creates an inherent decline in the accuracy of detecting the low probability of genuine threats. SDT provides insight into both false alarms (i.e., benign events treated as threats) and misses (i.e., genuine threats missed) while providing recommendations for calibrating one's sensitivity to the base rate of threats and the potential consequences.

2.2 Resilience Theory and Its Application to Security

Resilience Studies have shifted from a limited focus on bouncing back from adversity, to a more comprehensive focus on how individuals and organizations adapt positively during challenging times. Resilience Theory offers important insight into the following concepts in relation to Security:
Psychological Resilience includes the dynamic process of positively adapting during times of extreme adversity. Some of the key psychological factors contributing to this type of resilience are developing Self-Efficacy, Optimism, Cognition Flexibility and Emotional Regulation. In relation to the world of Security, Psychological Resilience allows for individuals to continue to act within the confines of what is appropriate security behavior, despite the sophistication of the social engineering they are experiencing; to be vigilant while carrying out routine tasks even knowing that routines may not create opportunities for vigilant behavior; and to constructively recover from security breaches.

Organizational Resilience focuses on the difference between these psychological concepts at the individual level, to the organization's collective ability to anticipate, prepare, react to, and adapt to, both gradual and sudden disruptions. Organizations classified as "High-Reliability Organizations" (HROs) operate in high hazard environments such as Aviation and Nuclear Power, successfully maintain safe environments for all Accomplished through an awareness of Collective

Mindfulness, Deference to Expertise, and a Commitment to Resilience. Similarly to HROs, the organizational resilience associated with Security requires organizations to develop these abilities in a collective manner and coordinated response to External Threats.

Ecological Resilience Models explain how systems possess certain properties that allow them to continue functioning despite disruptions or changes. Ecological Resilience Models distinguish between Engineering Resilience (a system's ability to return to a stable state after a disruptive event); Ecological (a system's ability to retain its function/identity despite changes in its contextual environment); Evolutionary (a system's ability to undergo a transformative change as it adapts and changes). In relation to Security, this implies that we must begin to look past the traditional Engineering Recovery Model (the bounce-back model) and begin incorporating "Adaptive Learning" processes (building upon your mistakes and incidents).

The Psychological Capital (PsyCap) theory from positive organizational behavior presents a useful framework for reconceptualising human security assets. PsyCap consists of four psychological resources that can be measured:

Self-Efficiency: the belief in one's capacity to successfully perform particular tasks. One's security self-efficacy would include the ability to identify potential threats, to follow established protocols, and to make corrective as well as preventative security decisions.
Hope: the combination of knowing what goals you want to achieve and how to achieve them, along with the personal empowerment to pursue those goals. Security hope refers to being aware of what security goals are in your organization, and believing that there are realistic ways to achieve those goals.
Optimism: a tendency to view all experiences of success (past, present, and future) positively. Security optimism helps keep employees engaged throughout the life cycle of a security organization and in the face of failures that frequently occur in security and with some departments in any security organization.
Resilience: the ability to recover from negative experiences (adversity, loss, etc.) and/or to grow from them. Security resilience helps individuals recover from their mistakes in security without being forced into a less engaged, defensive, or detached state of being toward their security responsibilities.

The PsyCap Theory demonstrates that these four resources can either be thought of as state-like (they can be changed or developed through a training intervention, etc.) rather than trait-like (i.e., fixed, inherent attributes) and demonstrate strong reliability in their measurement and significantly predict several important outcomes (performance, satisfaction, etc.) regarding employees and organizations.

The theoretical evidence supporting the development of employee security competence as a psychological capital (PsyCap) is significant based on the PsyCap Theory of Positive Organizational Behavior.

Motivation as it relates to Self-Determination Theory (SDT)

The Self-Determination Theory (SDT) distinguishes between intrinsic motivation (doing things just because you are interested in them) and extrinsic motivation (doing something for someone else for an incentive).

III. PREPARE YOUR PAPER BEFORE STYLING

3. Cognitive Resilience Framework for Cyber Security

3.1 Overview of Framework and Core Constructs

The Cognitive Resilience Framework for Cyber Security guides the conceptualization of human security competence as multidimensional psychological capital, consisting of four interrelated yet distinct dimensions:

Security Self-Efficacy (SSE): The degree of confidence a person has in their capability to identify security threats, apply appropriate protective behaviors, and effectively contribute to organizational security.
Threat Vigilance Capacity: The capacity to sustain appropriate attention to security-relevant cues in the presence of routine, competing demands, and low threat base rates.

Decision Making Resilience (DMR): The capability to make security-appropriate decisions in a situation of uncertainty, time pressure, social influence, and cognitive overload.
ARC-Adaptive Recovery Capacity: The degree to which one learns constructively from security errors, recovers psychological equilibrium after incidents, and contributes to organizational security learning.
All these in combination form a higher order construct referred to as Cognitive Security Resilience, which is psychological competence of an individual in sustaining appropriate security behaviors across varied and challenging contexts.
3.2 Dimension 1: Security Self-efficacy Security self-efficacy extends Bandura's self-efficacy construct into the security domain. We define SSE as a person's judgment of their capability to identify security threats, execute prescribed security behaviors, and make appropriate security decisions across typical and challenging situations they encounter in their organizational role. Theoretical Properties: SSE is domain-specific rather than general-one may have high efficacy for physical security but low efficacy for data classification decisions. It is also task-specific within the security domain. Someone may feel confident identifying phishing emails, but may be uncertain about secure password management. SSE operates through four psychological mechanisms:
Cognitive: Influences attention to security-relevant information, information processing, and the analytical effort invested in security decisions
Motivational Data: Impacts security goal choice, effort exerted, and persistence through difficulty
Affective: Relieves anxiety and stress associated with security responsibilities
Selection: Guides whether people approach or avoid security-relevant situations

Sources of Security Self-Efficacy:
Following self-efficacy theory, SSE is developed through four-sources:
Mastery Experiences: Performance of security behaviors will build efficacy most powerfully. For this, there has to be real opportunities to practice security skills along with feedback. Vicarious experiences include observing similar others successfully performing security behaviors-security role models and peer success stories. Social Persuasion: Credible others expressing confidence in one's security capabilities via manager support, peer recognition. Physiological/Affective States: Reduction of anxiety, stress management in security contexts.
Prospective Benefits Of Security Self-Efficacy According To Theory, There Is A Correlation Between The Increase Of

Security Self-Efficacy (SSE) And Increased Participation In Security-Oriented Activities Steadfastness In Supporting The Ability To Follow Complex Processes In Security Better Performance Of Security Under Pressure Increased Positive Security Behavior Beyond Minimal Compliance More Openness To Disclosing Security Issues

3.3 Dimensional Orientation 2; Threat Vigilance Capacity Threat Vigilance Capacity: The Amount Of Cognitive Capability To Sustain Appropriate Amounts Of Security Attentiveness Through The Normal Barriers Which Are Present To Sustain Attentiveness. This Dimension Utilizes But Extends Existing Vigilance Research To Reflect Unique Security Challenges. Theoretical Components; Threat Vigilance Capacity Has Three Subcomponents; Sustained Attentional Capability: The Ability To Sustain Attention On Security-Relevant Cues Over Extended Time Frame Without Experiencing A Significant Drop In Performance. Contextual Discrimination: The Ability To Identify |Identify Small Contextual Anomaly As Related To Security For Security-Related Components In Common Areas; Adaptive Scanning: An Ability To Change The Distribution Of Security Attention To Meet Both Situational Risks And Task Requirement.
Cognitive
Mechanisms:There are four cognitive mechanisms that TVC operates through:**Selective attention:** The ability to filter the security-relevant information from the irrelevant information without creating an overload of false alarms.
Divided attention: The ability to be aware of security threats while performing the primary task.
Executive control: Putting away the automatic responses when you discover an anomaly that may indicate security threat-related activity.
Pattern recognition: Noticing the "deviations" from a pattern that may indicate a threat Influences on Threat Vigilance:-TVC may vary due to Differences between individuals in their ability to use attentional control and working memory Availability of cognitive resources at a time (i.e., fatigue, cognitive load)
The design and arrangement of the environment (i.e., salience of the security cues and the signal-to-noise ratio) Motivation and perceived likelihood of being threatened Previous training and development of schemas regarding the threats and how they may develop.

Theoretical Underpinning layer of the DMR dimension is a perception of how security often compromises the judgement required to make an appropriate security decision.

Theoretical Underpinning of the DMR dimension is based on the fact that Security Decisions are made under decision-improving non-security related conditions such as;

3.4-Decision-Making Urgency; The need for a Decisions immediate response creates a pressure to quickly reach a decision.

-Decision-Making Uncertainty; Decisions are always based on information available before reaching a decision.

-Decision-Making Social Influence; Social norms can often affect the judgement of the decision-maker.

-Decision-Making Cognitive Depletion; Decisions made when the individual's cognitive load is at or near the maximum.

-Decision-Making Emotional State; Fear and stress can alter the normal cognitive ability of the decision maker.Several mechanisms through which Psychological Resilience (DMR) is able to support decision-making quality in the face of challenges include Cognitive Mechanisms, such as:

Cognitive Mechanisms:
Meta-Awareness--Recognizing the existence of suboptimal decision conditions
Compensatory Strategies--Activating deliberative processing when automatic responses are not reliable
Heuristic Management--Recognizing when intuitive processes are subject to manipulation
Cognitive Flexibility--Adjusting decision-making strategies based on situational context

Psychological Resilience (DMR) is also supported by:

Protective Factors:
Well-developed decision schemas for common security scenarios
Awareness of one's unique vulnerability patterns (the circumstances in which one's judgment is most likely to fail)
Pre-determined decision rules for high-risk situations
Psychological distance techniques (e.g., depersonalization) to alleviate the impact of social pressure
The ability to regulate emotions

As a result of having High Decision-Making Resilience (DMR):

More Consistent Security-Appropriate Decisions can be made Across Different Contexts
Less Susceptibility to Social Engineering Manipulation
Better Decision-Making Under Pressure and Uncertainty
Fewer Security Errors as a Result of Judgment Failures
Higher Level of Confidence in Security Decision-Making

3.5 Adaptive Recovery Capacity (dimension 4)
The Adaptive Recovery Capacity (ARC) is defined as a psychological competence to react positively to the events of the security failure or incidents. An individual's own recovery and organization's learning and recovery is included in this dimension. The ARC dimension takes into account research on resilience and error management.

Theoretical Components of the ARC
The ARC is made up of three major but interrelated capabilities:

1. Psychological Recovery – Returns the individual to a functional psychological condition after the events of a security failure or incident without feeling shame, anxiety or defensiveness.
2. Cognitive Reframing – The individual views the event(s) of security error(s) as a learning experience instead of a fixed failure with permanent implications to self-image.
3. Contributions to Learning – The individual remains actively engaged in learning from their security error(s) by providing the lessons they have learned to others in their organization, with a view to preventing future security errors that may occur.

Behavioral Mechanisms by Which Adaptive Recovery Capacity (ARC) Operates

The behavior of the ARC is accomplished through several psychological processes:

1. Attribution Patterns – Individuals make unstable, specific, external attributions for their security error(s), as opposed to using global, stable, internal attributions that undermine their self-efficacy.
2. Emotional Regulation – Individuals manage their feelings of shame and guilt and anxiety concerning incorrect behavior (defensiveness) by controlling these emotions.
3. Growth Mindset – Individuals view their ability in security competence as having the potential to be developed, rather than being fixed.
4. Psychological Safety – Individuals feel that if they disclose their security errors, they will be supported rather than punished.
The Contextual Influences Affecting the Also Include Relationship with The Activity:
1) The Error Culture(A culture that views errors as opportunities for learning or as an indicator of incompetence), which is influenced by how both peers and managers respond to errors when they are reported by employees.
2) All learning systems that support the error-based learning in organizations must also be taken into account.
3) The Psychological Safety Climate: The general level of accepted risk within an organization for interpersonal risk-taking.

Higher levels of Adaptive Recovery (ARC), which is to a greater extent what happens with an increased level of ARC:

1) The shorter time taken to return to effective functioning after making an error.
2) The increased rate of reporting and disclosing errors by employees, thus, an increase in the amount of learning from security incidents.
3) The decreased possibility of making the same error again.
4) Increased collective organizational learning.

Theoretical distinctions are made between the four dimensions of the CRFCS, but these dimensions are interrelated Functionally. There are several relationships among the four dimensions of the CRFCS that we found through a review of the literature on self-efficacy.
SSE ↔ TVC: The individual experiences anxiety when faced with tasks requiring vigilance; they are more likely to be anxious when under pressure. Self-efficacy increases the ability to sustain vigilance by decreasing anxiety, thus allowing the individual to have greater confidence that vigilance will result in successful threat detection. By experiencing successful threat detection, the individual develops self-efficacy.
SSE ↔ DMR: An increase in self-efficacy enables an individual to engage in deliberative processing while under pressure. Individuals who consistently make high-quality decisions build on self-efficacy.
DMR ↔ TVC: When a person is resilient to making poor decisions, he/she continues to have a capacity for vigilance. Continual engagement in effective vigilance increases the likelihood of making high-quality decisions.
ARC → SSE: An individual who recovers effectively from errors and contributes successfully to learning opportunities rebuilds their sense of self-efficacy that was diminished due to error experiences.
ARC → DMR: When an individual learns from prior decision-making errors, he/she is able to improve decision-making quality when at similar conditions.
Overall, relationships among the dimensions indicate that development interventions directed towards one of the dimensions may yield positive results toward developing other dimensions; however, deficiencies in one dimension may hinder the development of the other dimensions.

4. Theoretical Propositions: Antecedents, Mechanisms, and Outcomes

4.1 Individual-Level Antecedents

We propose several categories of individual differences as antecedents to Cognitive Security Resilience:
Proposition 1 (Cognitive Capabilities): Individual differences in working memory capacity, attention control, and executive function enhance Cognitive Security Resilience, particularly for the TVC and DMR dimensions.
Proposition 2 (Personality Characteristics): Conscientiousness and emotional stability positively influence overall CSR. Openness to experience facilitates ARC by providing a way for individuals to develop a learning orientation. Agreeableness has a complex relationship with CSR by providing the potential to increase the individual's ability to seek help, thus improving SSE, while also increasing an individual's vulnerability to the influence of others through DMR.
Proposition 3 (Motivation): An individual with intrinsic motivation (i.e., autonomous) for security is likely to have a greater CSR level than someone whose motivation is based on external factors (i.e., controlled). An individual who has internalized their security values will be more sustainable in their CSR over time and in different situations.
Proposition 4 (Experience): An individual's experience related to security (i.e., before being trained, exposure to an incident, working in the security field) creates a curvilinear relationship with CSR—an individual with a moderate level of security-related experience has the greatest resilience, while an individual with minimal experience has the lowest level of competence and an individual with significant security experience may develop cynicism or fatigue.
Proposition 5 (Metacognitive Awareness): Higher levels of metacognitive awareness (having a better understanding of what one is thinking and what one can and cannot do and how to compensate for limitations) positively impacts DMR and TVC, in that higher levels of metacognitive awareness enhance an individual's ability to self-monitor and activate compensatory strategies.

4.2 Organizational Level Antecedents

Proposition (Psychological Safety): The Organizational Psychological Safety Climate negatively impacts all of the CSR Dimensions, with the greatest impact seen on ARC. The Psychological Safety Climate allows for error disclosure, seeking assistance, experimentation, etc. (all of which are critical to developing capabilities).

2.7 Organizational Learning Systems

The Organizational Learning System supports the organization in continually improving and developing its security capabilities, through the collection of security lessons learned and the dissemination of that information to the workforce via both Leadership and Employee level interaction and collaboration.

2.8 Security Technology Usability

The Organizational Security Technology Usability Model provides a framework for examining the unique characteristics and capabilities of each of the Security Technologies, and for determining how those technologies will affect workflow and Productivity, while minimizing the cognitive burden on the employee, through a variety of methods.

2.9 Security Role Clarity

Having a well-defined understanding of security expectations, roles, and responsibilities positively affect how effectively an organization achieves its SSE and DMR objectives. When these roles are ambiguous, it can negatively impact the organization's ability to effectively perform Security-Related Tasks and make effective decisions based on Security-Related Factors.

4.3 Developmental Mechanisms

Proposition 11 (Mastery Experience Pathway): Engaging in authentic experiences that provide practical complexity and meaningful feedback will be the most effective way to develop CSR, and the development of CSR will be driven through the development of self-efficacy and developing schemas.

Proposition 12 (Social Learning Pathway): The presence of credible role models (peers, leaders, champions) facilitates the enhancement of a person's CSR through vicarious learning. This proposition applies more strongly to individuals with lower levels of self-efficacy.

Proposition 13 (Development of Cognitive Skills): As individuals develop their skills related to cognitive skill sets associated with security, such as threat pattern recognition, decision analysis, and attention management, they can build CSR through additional pathways other than just knowledge acquisition.

Proposition 14 (Reflective Practice): By reflecting on their own security-related experiences, decisions, and the outcomes of their actions, individuals can strengthen their CSR (especially ARC and DMR) through developing metacognitive skills and elaborating on their schemas through structured reflection.

Proposition 15 (Incremental Challenge): Gradually increasing levels of challenge regarding task complexity helps reinforce and strengthen an individual's CSR abilities. When an individual is challenged with excessively complicated materials, their ability to maintain self-efficacy in the area of security is undermined; however, if they are provided with less challenging materials, an individual's ability to build a sense of competence concerning security will suffer.

Section 4.4 describes mediating mechanisms concerning CSR and security performance. These mechanisms are described in the following Propositions.

P16. CSR has a partial effect on security performance by influencing where an individual allocates his/her attention. The increased ability to provide an appropriate level of attention to security is balanced with an appropriate level of employee productivity.

P17. CSR assists in using cognitive resources more effectively through the automation of responses to routine security incidents while providing an outlet for employees to make a decision regarding the allocation of their cognitive resources to a more complex and/or uncertain situation.

P18. The increased level of CSR leads to less anxiety regarding security issues and prevents the degradation of employee performance due to increased stress levels.

P19. CSR assists in predicting the appropriate help-seeking behavior of employees in relation to less-familiar security scenarios. Low levels of efficacy lead to both a higher tendency for excessive (learned helplessness) help-seeking and a lower tendency for sufficient (covering mistakes) help-seeking.

P20. CSR will influence the way in which an individual processes security-related information. Higher levels of CSR provide individuals with the ability to systematically process and resist attempts at persuasion. In addition, higher levels of CSR promote the ability to detect contradictions within information.

4.5 Outcome Predictions

Proposition 21 (Security Behavior Performance): CSR will have a positive relationship to objective security behavior performance (phishing, policy compliance, secure practices) with the potential for CSR to be maintained over time and across multiple contexts.

Proposition 22 (Proactive Security Behavior): CSR will predict security behaviors that go beyond what is expected of individuals in their roles (e.g., reporting threats, supporting peers and suggesting improvements to security procedures) with the greatest impact on those behaviors that are attributed to the SSE and ARC dimensions.

Proposition 23 (Error Recovery): Individuals with high CSR will be able to recover from security errors much faster and more completely than their counterparts who have lower CSR; therefore, secure practitioners will likely require less supervision or support to recover from their security mistakes than will those secure practitioners who have lower CSR.

Proposition 24 (Incident Contribution): Individuals with high levels of CSR are not likely to have as many involvement in the security incidents, and the positive impact of CSR on engaging in fewer and better security incident contributions will be partially mediated through the security behaviors performance, and thus partially through the effect of CSR on threat detection and decision quality.

Proposition 25 (Sustain Performance): CSR will predict that individuals will be able to maintain their level of security performance under difficult conditions such as high workloads or time pressures or in environments that are expected to lead to performance degradation by individuals with low CSR.

4.6 Factors That Impact Results

Proposition 26 (Task Complexity Moderation): The impact of CSR on individual performance increases when the individual is completing more complex security-related tasks. For example, routine or mediocre security-related tasks can be performed well by individuals with low levels of CSR; whereas, when entering into a complex security-related task environment CSR levels of individuals can be easily distinguished.

Proposition 27 (Threat Sophistication Moderation): The impact of CSR on threat detection increases when the

sophistication of the attack increases. For example, low-level attacks can be detected regardless of the level of CSR of the individual; however, sophisticated and well-crafted social engineering attacks can be used to distinguish between individuals with high CSR and low CSR.

Proposition 28 (Organizational Support Moderation): Organizational Security Support (i.e., technologies, processes, and culture) moderates the impact of CSR on organizational performance. Strong organizational Support can partially compensate for a lower level of CSR of individuals, however, weak organizational Support makes the ability of individual CSR to affect organizational performance substantially more important.

Proposition 29 (Role Risk Moderation): The importance of individual CSR is dependent on the organizational role of the individual, higher risk positions (e.g., executive access, authority over financial matters, and possession of sensitive data) tend to demonstrate a stronger relationship between CSR and performance than lower risk positions.

Proposition 30 (Recovery Support Moderation): Organizational Recovery Support (i.e., psychological safety and learning systems) moderates the impact of ARC; higher levels of ARC benefit from stronger Recovery Support systems than lower levels of ARC.

5. Measurement Considerations and Operationalisation

5.1 Measurement Difficulties

Theoretical and practical challenges presented by the Operationalization of Cognitive Security Resilience include:
Complexity of construct: The CSR includes many dimensions and therefore requires ways to measure both dimensional and totality of the CSR, but it also creates difficulties for respondents due to potentially imposing too much burden on them.
Specificity vs Generalizability - Security behaviors differ greatly by situation, so a measurement must provide enough specificity to allow for an actionable response while allowing for comparison across positions and organizations.
Desirability - Security competence includes qualities that people perceive as desirable, which could lead to overstating one's own ability when measuring. Thus, one must validate any self-report measurements against behaviorally based indicators.
Dynamics - Because CSR is a continually changing and evolving state, a measurement approach should separate stable individual differences from those that are capable of change.
Assessment of Actual Performance - The assessment of an organization's actual security performance encounters various difficulties that may include a low number of instances (occurring infrequently), the date a breach is discovered is months or even years after a compromise occurred, and that technical controls may mask human errors).

5.2 Proposed Measurement Methods

Self-Reported Psychometric Scales:
Well-designed scales measure CSR dimensions using validated items relating to the participants' perceptions of their capabilities, rather than measuring solely on the basis of what they know. Each dimension has a dedicated subscale:

SSE Scale: Items that measure the respondent's confidence in completing representative security tasks: e.g. "I can identify suspicious emails even when they look legitimate" (7-point Likert scale).

TVC Scale: Items that measure the respondent's perceived ability to be vigilant: e.g. "I pay attention to security risks while I am busy with other things."

DMR Scale: Items that measure the respondent's confidence in making decisions during times of stress: e.g. "Even under extreme pressure, I am capable of making sound security decisions."

ARC Scale: Items that measure the respondent's ability to recover and to learn from security mistakes: e.g. "When I make security mistakes, I learn something of tremendous value."

Scale development will follow psychometric standards, including expert review, cognitive interviews, pilot testing, and validation through factor analysis and convergent/discriminant validity assessments.

Controlled simulation assessments yield objective measures of performance:

Phishing Simulations: The detection rates of the various levels of phishing.

Decision Scenarios: Providing participants with realistic security dilemmas and measuring their decision-making abilities.

Vigilance Tasks: Sustaining attention to security events and measuring accuracy and ability to sustain vigilance over time.

Recovery Scenarios: Providing participants with the opportunities to learn and regulate emotions post-error.

While controlled simulations yield objective measures, they create an artificial environment and require considerable resources.

Behavioral Observations:
Directly observing an individual's security behaviors.
1) Compliance audits: the use of structured observations to determine the level of security compliance or practice adherence

2) Peer Ratings: the way that coworkers will evaluate individual's observed security behavior;

3) Manager Assessments: evaluations made by supervisor's that determine if someone has a sufficient level of competence around security

4) Critical Incident Analyses: when examining what type of behaviors were exhibited during cases when the individual was challenged by a real-world event related to security

While methods of observational approach have some level of ecological validity, there is also the potential for being intrusive, as well as resource intensive.

Physiological/neuropsychological Measurements: a variety of emerging offerings exist that use physiologic or neurophysiologic measures to identify types of underlying cognition:

Eye Tracking: for assessment of observer's visual focus over time as they complete tasks related to security.

Cognitive Task Performance (Executive function, Working Memory, Attention: For Assessment of executive functioning, working memory capacity, ability to sustain attention is found in the observables

Stress Response (physiological arousal) during the time of security decision-making

Neural Imaging: Assessment of brain activity (in research contexts) during times of associated security cognition

These approaches provide greater levels of objectivity than previously described approaches, but, at the same time, present significant limitations in terms of how they can practically be applied or scaled.

5.3 Multi-Method Assessment Strategy

The best way to evaluate CSR is through an approach that uses a ,

- **Initial Assessment:** Psychometric Scale - Establish Baseline CSR.
- **Periodic Simulation:** Quarterly Behavioral Assessments to track progress of CSR development
- **Continuous Monitoring:** Unobtrusive Metrics (e.g., Phishing Click Rate, Report Behavior) to establish CSR activity.
- **Annual Comprehensive Evaluation:** Multi-source Ratings, Simulation, and Self-Assessment to get a complete picture of the company's CSR from all perspectives.

This approach to CSR combines the best assessment practices to give a just balance between depth of measurement and practicality.

5.4 Levels of Analysis of Corporate Social Responsibility

CSR can be analysed at three (3) distinct levels:

1. Individual Level - Individual CSR profiles are created to help the individual establish Development Plans and Role Assignments.
2. Team/Collective CSR - AR Programme would incorporate all members of the group/team to measure the Security Capability of the Team/Collective.
3. Organizational Level - Uses weighted distribution maps of all Employees CSR to assess the Human Security Capability and Vulnerability of the organization.

The analysis at all three levels also help explain the combined effect of CSR at the Individual, Team/Collective, and Organizational levels and how their interactions across levels impacts CSR outcomes.

Organizational Level Consequences - Cultural/CSR and Security Culture

6.1 Security Culture and CSR

The Organizational Security Culture defines the collective values, norms, and beliefs regarding security within an organization. It is a part of the overall culture of an organization.

CSR Can Be Defined By Culture: Organizations that have developed a Security Culture provide individuals with the opportunity to develop CSR through socialisation, modelling, and resources. The Security Climate created by the Organizational Security Culture enables individuals to Develop CSR.

CSR Can Create A Security Culture By Creating Norms: When many individuals develop High CSR, the collective Norm is to engage in Security-Positive Behavior. Individuals with High CSR Become Cultural Carriers by influencing People and establishing Standards of Behavior.

CSR and Security Culture Exchange: The relationship between Individual CSR and Organizational Culture is Reciprocal; the Culture develops the Individual's Capability, and the Total Individual Capabilities determine the Culture.

Given this perspective, Developing Security Culture requires simultaneous focus on Developing Capability (to Develop CSR) and Changing Climate (to Develop a Security Culture.)

6.2 Strategic Management of Human Security Assets

When organizations view CSR as an Asset, they can use Strategic Management to manage Human Security Assets. Strategic Management can be viewed in three parts:
Identifying Assets: A Workforce CSR Assessment can Identify Individuals with High Capability for Security Related Jobs, and Individuals at High-Risk that require Additional Development Support.
Developing Assets: By Treating CSR as an Asset, you can Create Development Programs, and Calculate ROI Based on Incident Reduction Rates, Quicker Identification of Threats and Increased Agility in Security.
Allocating Assets: You should Align Individuals' CSR Profiles to the Job which they hold.

Strategies for Differentiated Development (6.3)
Personalized development strategies are made possible through the CSR framework. Different strategies may be pursued by individuals based on multiple dimensions of CSR.
Targeting of Deficit: Individuals who have low SSE but have adequate capacity in all other dimensions will benefit from having experience in the mastery experience(s) as a means of building confidence.
Leverage of Strength: Individuals who score high on the CSR scale will require less training volume, however through advanced challenge and leadership development opportunities, they may benefit from additional support for growth.
Interventions Based on Each Dimension: Individuals who are weak in the TVC dimension require assistance with attention management training; individuals who are weak in the DMR dimension require decision-making simulation training; individuals who require ARC development, require psychological safety and reflective practice.

Prioritization of CSR Development based on Role: Different roles require emphasis on different CSR dimensions — for executives, strong DMR is needed for high-stakes decisions; for SOC analysts, strong TVC is needed for sustained vigilance.
Implications of Leadership (6.4)
CSR development through leaders:
Role Modeling: Leaders who demonstrate a visible CSR will model effective security behaviors; creating opportunities for individuals to learn vicariously, thus providing a powerful tool for creating a safe environment.
Creating a Climate for CSR: Leaders create psychological safety, resource availability, and priorities that will enable or constrain CSR development.
Setting of Expectations: By creating clear and reasonable expectations in the area of security, and providing developmental support, leaders can optimise the capability of an individual developing a CSR.
Facilitating Recovery: Leaders' response to security errors will have a significant impact on ARC development. Constructive responses and learning opportunities can help build capacity; in contrast, a focus on blame can hinder development.
Designing Recognition Systems: Leaders need to design recognition and reward systems that will either promote CSR development (i.e., intrinsic motivation, competence, and improvement) or detract from CSR development (i.e., focus on punishment, and expectation for perfection).

7 Future work

Theoretical Limitations and Future Research Directions
Current Limitations of the Framework
Theoretical Constraints: The Cognitive, Psychological, and Social (CRFCS) theoretical model focuses specifically on cognitive, and psychological (behavior), while also be inclusive of the influence of social structural components (ie., power, inequalities, politics) on security based behaviors. However, it does not provide enough of an integration into the theoretical framework.

Cultural Generalizability of the Framework: Most of the framework development is based upon Western theoretical principles and requires validation across cultures where cultural differences in autonomy, authority, and error handling may impact culture-specific behaviors.

IV. 8. Conclusion

Cognitive Resilience Framework for Cyber Security introduces a theoretical framework which shifts focus from a deficit-based, reactive approach to creating capabilities. Theoretical Framework Labelling Human Security Competence as a multidimensional cognitive resilience which includes: self-efficacy, vigilance capacity, decision resilience and adaptive recovery, creates a basis for developing more human-centric security approaches. The framework merges well-established theories of Psychology and Security into Cognitive Security Resilience by offering for empirically testing antecedents, mechanisms, and outcomes which occur due to developing Cognitive Security Resilience. Understanding Cognitive Security Resilience creates opportunities for the organization to assess its current security practices and shift to new methods that value the investment into developing Cognitive Security Resilience as much as building and supporting the technical aspects of their security program, leading to a holistic view of security in the organization where all areas contribute to improved security. Organizations that are aware of and actively cultivate cognitive security resilience as a Strategic Psychological Capital will have better security outcomes than Organizations that rely on the traditional compliance based awareness of their security an organization has towards its security program, thus eliminating the human element as "the weakest link" in the organizations overall cybersecurity posture, if they go through the same development process for their Human Security Capability as they do for their Technical Security Infrastructure.

V. References

Bandura, A. (1997). Self-efficacy: The exercise of control. W.H. Freeman and Company.
Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523-548.
Cialdini, R. B. (2006). Influence: The psychology of persuasion. Harper Business.
Deci, E. L., & Ryan, R. M. (2000). The "what" and "why" of goal pursuits: Human needs and the self-determination of behavior. Psychological Inquiry, 11(4), 227-268.
Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. Human Factors, 37(1), 32-64.
Evans, J. S. B. T., & Stanovich, K. E. (2013). Dual-process theories of higher cognition: Advancing the debate. Perspectives on Psychological Science, 8(3), 223-241.
Frazier, M. L., Fainshmidt, S., Klinger, R. L., Pezeshkan, A., & Vracheva, V. (2017). Psychological safety: A meta-analytic review and extension. Personnel Psychology, 70(1), 113-165.
Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. Computers & Security, 31(8), 983-988.
Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviors. Heliyon, 3(7), e00346.
Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31(1), 83-95.
Kahneman, D. (2011). Thinking, fast and slow. Farrar, Straus and Giroux.
Luthans, F., Youssef, C. M., & Avolio, B. J. (2007). Psychological capital: Developing the human competitive edge. Oxford University Press.
Masten, A. S., & Reed, M. G. J. (2002). Resilience in development. In C. R. Snyder & S. J. Lopez (Eds.), Handbook of positive psychology (pp. 74-88). Oxford University Press.
McCormac, A., Zwicki, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. Computers in Human Behavior, 69, 151-156.
Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165-176.
Rosenstock, I. M., Strecher, V. J., & Becker, M. H. (1988). Social learning theory and the health belief model. Health Education Quarterly, 15(2), 175-183.
Schein, E. H. (2010). Organizational culture and leadership (4th ed.). Jossey-Bass.

Simon, H. A. (1972). Theories of bounded rationality. In C. B. McGuire & R. Radner (Eds.), Decision and organization (pp. 161-176). North-Holland Publishing Company.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487-502.

Sweller, J., van Merriënboer, J. J. G., & Paas, F. (2019). Cognitive architecture and instructional design: 20 years later. Educational Psychology Review, 31(2), 261-292.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. Information & Management, 49(3-4), 190-198.

Weick, K. E., & Sutcliffe, K. M. (2007). Managing the unexpected: Resilient performance in an age of uncertainty (2nd ed.). Jossey-Bass.

Zimmerman, B. J. (2000). Self-efficacy: An essential motive to learn. Contemporary Educational Psychology, 25(1), 82-91.