8-1-2019

# Thriving Cybersecurity Professionals: Building a Resilient Workforce and Psychological Safety in the Federal Government

Rephael Houston
*University of Pennsylvania*

# Thriving Cybersecurity Professionals: Building a Resilient Workforce and Psychological Safety in the Federal Government

**Abstract**
Cybersecurity professionals in the federal government work on complex problems in organizations where they have multiple competing roles. In addition, the gap between workers with cyber skills and job openings means that current cybersecurity professionals must carry a heavy load. Combined, this can lead to stress that has negative consequences for their well-being. Positive psychology can help address this, particularly through enhancing positive experiences, leveraging character strengths, developing resilience skills, and building psychological safety. Resilience skills help cybersecurity professionals increase capacity their capacity to deal with uncertainty and build strong teams. Psychological safety supports and environment of innovation and professional development. These strategies are accessible ways for cybersecurity professionals to thrive in their work, improving their well-being as well as their ability to better address the emergent threats of a volatile world.

`

**Keywords**
active constructive response, capitalization, character strengths, cognitive behavioral therapy, cognitive bias, cybersecurity, psychological safety, public service, resilience

**Disciplines**
Defense and Security Studies | Information Security | Leadership Studies | Organization Development | Public Administration

# Thriving Cybersecurity Professionals:

# Building a Resilient Workforce and Psychological Safety in the Federal Government

Rephael Houston

University of Pennsylvania

A Capstone Project Submitted

In Partial Fulfillment of the Requirements for the Degree of

Master of Applied Positive Psychology

Advisor: B.J. Jones

August 1, 2019

# Thriving Cybersecurity Professionals: Building a Resilient Workforce and Psychological Safety in the Federal Government

Rephael Houston
thrivingprofessionals@gmail.com

Capstone Project
Master of Applied Positive Psychology
University of Pennsylvania
Advisor: B.J. Jones
August 1, 2019

## Abstract

Cybersecurity professionals in the federal government work on complex problems in organizations where they have multiple competing roles. In addition, the gap between workers with cyber skills and job openings means that current cybersecurity professionals must carry a heavy load. Combined, this can lead to stress that has negative consequences for their well-being. Positive psychology can help address this, particularly through enhancing positive experiences, leveraging character strengths, developing resilience skills, and building psychological safety. Resilience skills help cybersecurity professionals increase capacity their capacity to deal with uncertainty and build strong teams. Psychological safety supports and environment of innovation and professional development. These strategies are accessible ways for cybersecurity professionals to thrive in their work, improving their well-being as well as their ability to better address the emergent threats of a volatile world.

*Keywords:* active constructive response, capitalization, character strengths, cognitive behavioral therapy, cognitive bias, cybersecurity, psychological safety, public service, resilience

**Acknowledgements**

I am grateful for the constant love and support of my wife, Samiha Sobhan, who has encouraged me through every step of this process. In addition, I am thankful for my parents Larry and Joyce Houston for always helping me to learn and explore. I also appreciate all the critical figures across my academic and professional life that have allowed me to think and grow. My undergraduate advisor Anthony Blasingame, Ph.D., for encouraging me to always challenge myself at the University of Maryland at College Park. Sue Briggs, Ph.D., the founding director of the CIVICUS Living and Learning Program at the University of Maryland, for showing me how to stay actively engaged in service to the community. Maria Trujillo, Ph.D. faculty director and associate professor of the practice for the Master's in Systems Engineering and Master's in Technology Management at Georgetown University for demonstrating in word and deed what academic excellence is and how to embody "Cura Personalis." Leaders in the US Navy that showed me how to support individual thriving before I knew of positive psychology, including retired Captain Buzz Sorce, Captain Bruce Schutte, and retired Chief Warrant Officer Richard Lute, US Navy. Your examples are ones that I strive to follow. For my managers, Kevin Piekarski and Paul Dillmuth for giving me the freedom to put some of these ideas into practice. I am especially grateful for B.J. Jones for not only encouraging me to apply to the MAPP program but for graciously advising this capstone. To my MAPP.14, you are all an endless stream of wisdom and support. Thank you to the MAPP faculty and staff, you have given all of us the freedom to spread our wings!

Table of Contents

## Introduction

The internet helps us organize our work, social life, finances, and so much more -- and we are heavily reliant on its security as a result. The internet is no longer merely a global network of computers; it is the backbone of most of the modern world. Since its development by the Defense Advanced Research Projects Agency (DARPA) in the 1960s, the internet was designed to withstand nuclear war, so that it will keep working even when many of its parts are destroyed by even the most massive catastrophe (Mowery & Simcoe, 2002). The internet does not just face threats from outside forces; it is the very users (countries, terrorists, criminals, pranksters) of the internet who can steal or destroy data, networks, and systems. The US Army War College describes the current geopolitical world as filled with volatility, uncertainty, complexity, and ambiguity, or VUCA (Stiehm, 2002), which is increasingly evident in cyberattacks. A recent Executive Order 13870 (2019) on America's Cybersecurity Workforce focuses on providing agencies with increased flexibility to hire and reassign cybersecurity professionals to address these issues. The order comes out of years of shaping the cybersecurity workforce through the National Cyber Strategy, the President's 2018 Management Agenda, and Executive Order 13800 on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (Executive Order No. 13870, 2019). There are also efforts to improve cyber workforce training as well as change compensation that have bipartisan agreement (Lee, 2019). The need to change and support the cyber workforce is uncontroversial but focusing only on areas that are lacking leaves a lot of valuable human contributions unnoticed by the federal cyber workforce and does not harness their potential.

Recently, in Taiwan, the government tested whether incentive pay would increase public service motivation. The results have shown that public service motivation does not come through

compensation (Hsieh, 2018). Hsieh suggests that using the self-interest motivation (compensation) to increase engagement reduces public service motivation, which is something to be closely monitored. Workers must be paid fairly, and the public interest must always come first.

This paper seeks to help illustrate how positive psychology and related strategies can help enhance cybersecurity professionals' experiences and their contributions. Many of the hypothetical examples provided throughout this paper are based on my own experiences in this field. The first section will present an overview of the cybersecurity field, with a focus on roles and responsibilities. Next, a summary of the field of positive psychology will help illustrate why focusing on well-being is important. The third section will detail how positive experiences and traits come into play in a cybersecurity professional's experience. The following sections will then highlight resiliency and psychological safety strategies. These theories and tools will help illustrate how to create a stronger workforce in a cybersecurity environment - one that values competence as well as well-being.

**Role of the Cybersecurity Professional**

Every day, cybersecurity professionals: analyze cybersecurity information and establish its usefulness; collect intelligence information; operate tools to deny access to sensitive information; deceive adversaries into attacking mock systems and information; investigate cybersecurity crimes or events; operate and maintain information technology that adheres to high standards of security; protect and defend internal information technology networks and systems; securely provision information technologies that are designed and built with cybersecurity in mind; and oversee and govern organizations so that people within them can effectively do their

jobs (Newhouse et al., 2017). The work of cybersecurity professionals is broad and often team-based.

For example, the work to procure and develop cybersecurity systems takes dozens of people to conceptualize the needs of the agency, design what the system should do, solicit proposals from vendors, evaluate the bids, make selections of best offerors, and then support building the intended designed system and/or network (Newhouse et al., 2017; Federal Acquisition Regulation, 2019). Each phase of this procurement process may need the expertise of various types of cybersecurity expertise from system architects to lawyers (Newhouse et al., 2017). Cybersecurity professionals assist in even the early stages of writing the request for proposals (RFPs) to ensure the proper language and technical specifications are written into the proposals. Translating the functional requirements into a technical solution often takes the work cybersecurity professionals. Project managers use their cybersecurity expertise to develop timelines based on the agency's recommended technical solution and other factors. Software developers will use the best practices in security to create systems and applications that do not include security holes. Testers will perform security scans and evaluate compliance with documented specifications to validate that the work is both secure and meets the needs of the agency. Across the whole process, risk managers will take into account internal and external users' perspectives to ensure that compliance with regulatory standards is maintained, and notify senior leaders about mitigation strategies as well as unavoidable issues.

Beyond this important work, often what comes to mind with cybersecurity is maintaining confidentiality (only the correct users have access), integrity (the system or data is not altered), and availability (the system is ready to be used when it is needed) of a given system. But the form such work takes is not always technical in nature and can be more about processing forms

(Privacy and Paperwork Reduction Act compliance) more than monitoring systems (Gibson, 2015). The National Initiative for Cybersecurity Education NICE Framework (Newhouse et al., 2017) identifies a myriad of tasks that require cybersecurity professionals' critical knowledge and skills to secure data and networks. These tasks include, but are not limited to, answering requests for information; developing data standards, policies, and procedures; coordinating incident response functions; conducting Privacy Impact Assessments (PIAs) of the application's security design for the appropriate security controls; monitoring and reporting on validated threat activities; and recording and managing test data (Newhouse et al., 2017). There are over 1,000 diverse tasks cybersecurity professionals are assigned to do (Newhouse et al., 2017).

For the purpose of this paper, several roles will be illustrated to demonstrate the cybersecurity professionals' diverse responsibilities and work settings. In particular, a **digital forensics specialist** trains to uncover cybercrimes and provide support to criminal investigations. **All-sources analysts** use multiple intelligence collections methods to build a composite picture around what the evidence suggests. **Cyber operations planners** help develop and coordinate analyses to perform defensive or offensive missions. **Technical support specialists** are frontline workers ensuring that staff members have virus free computers and operational equipment. **IT project managers** ensure that the cost, scope, and schedule for an effort stays on track. **Information system security managers** document and monitor the implementation of an organization's cyber security program. All of these roles can benefit from the theories and strategies in this paper. To start, the next section will review developments in positive psychology to gain some background on the field and its applications.

## Positive Psychology

Although not formally developed until the late 1990s, positive psychology has origins in the post-World War II era. Humanistic psychology, developed by Abraham Maslow, sought to understand "healthy human being's functioning" (Buhler, 1971, p. 378) and how to enhance it. In his book, "Motivation and Personality," Maslow coined the term positive psychology (Maslow, 1954). Maslow's (1954) final chapter is "Toward a Positive Psychology" and describes how a new vision of psychology that borrows from the humanities, as well as other trends in psychology, could create a holistic psychology that does not only focus on what is wrong with humanity but seeks to support humanity's goodness.

Martin Seligman, in 1998, called for further development of positive psychology to focus on what makes human beings thrive (Seligman & Csikszentmihalyi, 2000). Seligman's call drew from various strands of research in subjective well-being, optimal experiences, positive emotions, and self-determination theory under one field of inquiry (Csikszentmihalyi, 1990; Diener, 1984; Fredrickson, 2013; Ryan & Deci, 2000). Positive psychology uses empirical research methods to answer questions of interest related to human flourishing, thus distinguishing itself from its humanistic psychology predecessors as well as from popular self-help guides (Duckworth, Steen, & Seligman, 2005).

Although it differs from past pursuits to understand what is human flourishing, positive psychology continues a tradition of searching for human thriving. Aristotle saw multiple paths to pursue a good life, so he thought humanity should focus our aims to ensure that we arrive at goodness (Melchert, 2002). He imagined a life of flourishing (eudaemonia) as one lived by reason in the pursuit of virtue (Melchert, 2002). Positive psychology seeks to help create a flourishing life by using models of well-being in pursuit of virtuous aims and means (Diener,

1984; Prilleltensky et al., 2015; Ryff, 1989). The field has three main areas of focus: positive experiences, character strengths, and positive institutions (Seligman & Csikszentmihalyi, 2000).

The first area, positive experiences, is captured in the PERMA model, which stands for positive emotions, engagement, relationships, meaning, and accomplishment (Seligman, 2013; Butler & Kern, 2016). Positive emotions have impact on increased immune response and increase in pain tolerance as well as increase overall wellbeing (Howell, Kern, & Lyubomirsky, 2007; Frederickson, 2001). Engagement is the effortful focus on a task that is enjoyable in the moment or "flow." Dedication over a long period is known as known as "grit" (Csikszentmihalyi, 1990; Duckworth, Peterson, Matthews, & Kelly, 2007). Relationships also play a protective role in supporting physical health as well as the ability to increase productivity by forming "high quality connections" with colleagues (Dutton, 2003;Tay, Tan, Diener, & Gonzalez, 2012). Making meaning creates a sense that individual lives matter and that they are connected to something greater than themselves (Steger, 2012). Accomplishment is being able to guide one's path toward fulfilling goals and gaining mastery (Ryan & Deci, 2000). All of the components of PERMA can be focused on separately, but also have been correlated to work together to increase well-being (Butler & Kern, 2016).

Character strengths are a common language to describe the qualities most valued across cultures that allow us to bring our most authentic best selves to any situation (Niemiec, 2018). Peterson and Seligman (2004) developed a list of 24 character strengths (Appendix B, table 1) after years of research looking at the most commonly valued traits in humanity. Strengths include kindness, creativity, love of learning, and humor (Appendix B). Years of further study have shown that knowing what our top character strengths (signature strengths) are can lead to increased well-being (Niemiec, 2018). Character strengths have been correlated with resilience

in a cross-sectional study that measured character strengths, resilience, and resilience-related factors (Martínez-Martí & Ruch, 2017). These studies are showing how important character strengths are to thriving.

The third component, positive institutions, has the potential to enable the best of humanity by creating pathways to support the other positive traits and positive emotions (Peterson, 2006). Though much of positive psychology's focus has been at the individual level, positive institutions are built on current understandings of positive experiences and traits. The best methods to create positive institutions can be found in the research of positive organizational scholarship, positive organizational behavior, and psychological capital (Cameron, Dutton, & Quinn, 2003; Luthans, 2002; Luthans & Youssef, 2004). Positive organizational scholarship is an umbrella term for the research efforts focused on thriving in the workplace (Cameron, Dutton, & Quinn, 2003). Positive organizational behavior focuses on developing interventions to support self-efficacy, hope, optimism, subjective well-being, and emotional intelligence (Luthans, 2002). Psychological capital takes the components of positive organizational behavior, and treats them like a resource to be measured and cultivated (Luthans & Youssef, 2004).

**Positive Experiences, Traits, and Cybersecurity**

With the many duties cybersecurity professionals in the government are called to perform under pressure, it may be hard to see how their work can include areas of thriving. When zooming in on cybersecurity professionals' individual roles, however, it becomes easier to see how cybersecurity professionals might have such positive experiences (Parker, Winslow, & Tetrick, 2016). It is through the lens of PERMA and use of character strengths that it becomes more apparent how cybersecurity professionals can thrive in their workplace (Seligman, 2013).

How do cybersecurity professionals find happiness in the age of WannaCry, the infamous ransomware case from 2017, that disrupted many businesses and government institutions such as the United Kingdom's National Health Services (Fruhlinger, 2018)?

**PERMA and Cybersecurity.**

Positive emotions are vital to human flourishing, as noted earlier (Frederickson, 2001). Positive emotions are not just visible expressions, but also biochemical responses that help humans to broaden their perspective of a situation and build the internal resources to pursue their goals (Fredrickson, 2001). The positive emotions of a digital forensics expert figuring out how to decrypt a data collection from a suspected hacker can be seen in a smile or a sense of joy. Even though a digital forensics specialist may have been working overtime for several weeks to better understand the digital artifacts of the famous WannaCry ransomware attack, for example, they still could have found excitement in their work by focusing on incremental insights they gain each day. Positive emotions can help sustain digital forensic experts in arduous tasks as well as find joy in their work.

Regarding engagement, a cyber operations planner could become fully immersed in validating data for hours, thus experiencing "flow." They may also need to sustain their efforts for months or years, demonstrating "grit" (Csikszentmihalyi, 1990; Duckworth, Peterson, Matthews, & Kelly, 2007). Cyber operations planners will want to thwart ransomware attacks like WannaCry. For example, a cyber operations planner could lose track of time as he or she tries to synthesize the latest intelligence about a cyber-attack and build contingency plans to respond to it. A cyber operations planner could also demonstrate grit, pursuing his or her passion and building perseverance to help integrate complicated defensive and offensive plans to mitigate or eliminate the capacity of an adversary's capabilities (Duckworth, Peterson,

Matthews, & Kelly, 2007). To support that engagement over time, the planner would have to deconflict plans with other agencies, develop administrative reports to pass to senior leaders, and learn to prioritize responses.

Cyber operations planners need grit to endure the long road until seeing some of their plans come to fruition (Duckworth, 2016). In prioritizing and making risk-based decisions, cyber operations planners could find flow in their daily activities because by creating a deliberate practice of focusing on routine tasks. Deliberate practice is one way to enter a state of "flow" (Csikszentmihalyi, 1990). Deliberate practice is uncomfortable, but flow sustains, so the more cybersecurity professionals practice their planning methodologies, the better they will get at sustaining flow and at their daily activities (Duckworth, 2016). Grit and flow alike drive cybersecurity professionals toward obtaining their goals, by helping them stay engaged.

Relationships come into play for cybersecurity professionals because they work in teams on complex problems all the time. For example, an all-source analyst needs to know their customers' decision-making needs and collaborate via virtual teams, while also supporting cyber planners, intelligence analysts, and collection managers. To find the instigators of the WannaCry attack, for example, it took many all-source analysts sifting through different pieces of the puzzle (Whitehouse, 2018). Relationships were an important part of being able to complete this important work. However, good social relationships are not just for getting the job done -- good social relationships have been shown to have a positive impact on individuals' health (Cohen, 2004). Creating good relationships for all-source analyses is not just about getting things done right. Creating trusting environments actually leads to more successful outcomes (Dutton, 2003; Edmonson, 1996).

Often, it is the work itself that can serve as a source of meaning to cybersecurity professionals. For example, technical support specialists are essential members of any cyber incident response. Technical support specialists are sometimes the first to hear ones to hear from users about attacks like WannaCry. However, often the vital role that these members play is obscured by how their work is organized through a "matrix team" where individual workers can find it hard to find meaning in some cases (Parker, Winslow, & Tetrick, 2016) Meaning is a basic human need and as a result, such a matrix structure can be problematic (Frankl, 1992; Von Devivere, 2018). Some technical support specialists develop a coherent story around why their role is valuable and see the larger purpose behind their routine tasks through the significance of doing their role well, such as being the frontline defenders of the network. Coherence, purpose, and significance are all essential elements of finding meaning (Martela, Martela, & Steger, 2016).

Other technical support specialists try to focus on tasks that help them highlight their purpose. What these cybersecurity professionals are doing is essentially "job crafting," which is figuring out what is the most valuable parts for the individual and finding how to do more of those tasks to support the organization (Wrzesniewski & Dutton, 2001). Meaning can also be developed through belonging (feeling part of a community), purpose (having goals that are larger than ourselves), storytelling (creating narratives that create a hopeful view of the world), and transcendence (feeling like we are woven into something more precious and more vast than ourselves) these elements sustain humans on their lives journeys (Smith, 2017). Cybersecurity professionals can create meaning out of their failures and successes, but also strive toward accomplishments.

Accomplishment, the final element in PERMA, is pursued for its own end (Seligman, 2013). The need to feel competent to achieve our goals is essential (Ryan & Deci, 2000). For instance, if an IT project manager (PM) were to hold team meetings to check the progress of restoring systems after the WannaCry attack, it would not be an accomplishment under this definition. However, if the PM was holding these meetings because they want to create an environment where the team felt heard and respected, that could be seen as an accomplishment. Trying to achieve better team cohesion as a goal in and of itself is very motivating to some PMs. People pursue goals that focus on hard to quantify qualities because they are focused on moving toward an internal standard and sense of mastery (Butler & Kern, 2016).

**Character Strengths and Cybersecurity.**

As discussed earlier, character also has a great impact on our well-being and, like PERMA elements, can be used in a cybersecurity environment. This paper will not discuss each of the 24 strengths, but it is worth highlighting how a few could come into play. Knowledge of one's character strengths isn't the only goal; cybersecurity professionals must also put their strengths into practice. Cybersecurity professionals can gain self-awareness from knowing who they are as individuals and magnify it when they put the best of who they are to work (Niemiec, 2018). Each character strength has unique ways to be unlocked. Cybersecurity professionals must then pay close attention to how they are using their strengths. When there is a good fit for how to employ character strengths, there is a "being" and "doing" alignment where a person's best self has fully engaged in an activity (Niemiec, 2018).

Picture a program manager (PM) who has the signature strengths of curiosity, gratitude, and zest (Niemiec, 2018). In their role, if the PM deliberately planned for opportunities to deploy her strengths throughout the day, she could have a more energetic and meaningful day. Curiosity

is diving into new experiences, searching for novelty, and being open to new adventures (Peterson & Seligman, 2004). For example, curiosity could mean that the PM is able to find the source of errors faster and come to resolutions to solve discrepancies. Gratitude is deliberately showing thanks when good things happen and being aware of things to be thankful for (Peterson & Seligman, 2004). The PM could show gratitude for having the opportunity to work on a special project that few of the opportunity to work on. Zest is having a desire to make the ordinary an adventure; treating everyday as special gift that is exciting; never giving less than the best effort in any endeavor (Peterson & Seligman, 2004).

Caution must be taken though to not under or overuse character strengths. The under and overuse of a character strength can have psychopathological consequences (Freidlan, Littman-Ovadia, & Niemiec, 2017; Grant & Schwartz, 2011; Seligman, 2015). For example, an appropriate amount of curiosity helps the PM stay thoughtfully engaged throughout the day. But while the underuse of curiosity looks like disinterest and can lead to others not feeling well regarded as well as not being fully engaged at the task at hand, the overuse of curiosity is nosiness, where attention is placed on gossip and hearsay in the workplace instead of working toward building relationships (Seligman, 2015). This overuse of curiosity can magnify problems.

Finding the optimal use of a cybersecurity professionals character strengths is an essential task and effortful process. Just as it is apparent when someone is over and under using a character strength, cybersecurity professionals have the ability to spot the goodness in others. If the PM started to look for the goodness in others “strength spotting” they would not only interact with others more effectively, but encourage others to be their best (Niemiec, 2018). We have the ability to bring the best of ourselves to the world each day. Yet, it is also important to have people around us that celebrate our triumphs.

This section illustrated how a cybersecurity professional can have positive experiences and advantage character strengths throughout their work. But as noted earlier, there are real challenges that must be contended with - ones that are often very significant. That is where resilience comes into play, as will be discussed in the next section.

## Resilience

### What is Resilience?

Resilience is about creating a new normal after setbacks that will enable a person to thrive (Bonanno, 2012; Reivich & Shatté, 2002; Reivich, Seligman, & McBride, 2011; Southwick, 2012). Most humans suffer setbacks and recover, thus making resilience the "ordinary magic" of the human experience (Masten, 2014, p. 3). However, although it is common to bounce back from hardships, it is not a process that should be left to chance. We can build resilience by increasing our protective factors in cyber security professionals facing a VUCA world of multiple threats to their organization and multiple roles they have to fulfill.

Protective factors are biology, connection, mental agility, optimism, belonging to a positive institution, self-mastery, self-awareness, self-regulation, and spirituality (Lopez et al., 2009). Some of these factors cybersecurity professionals are more easily influenced than others, such as heritable traits (Feder, Haglund, Wu, Southwick, & Charney, 2013). However, all protective factors can be enhanced, so there are ways to build resilience (Lopez et al., 2009). This section will focus on two strategies to help cybersecurity professionals build resilience: developing better stories to explain challenging events and bolstering connections at work through better communication.

**Better Stories.**

To increase our self-awareness and optimism, we can change the stories that we tell ourselves about the world we live in (Southwick, 2012; Seligman, 1991). The stories we have in our head dominate the way that we live our lives. Cybersecurity professionals can use methods of reframing to generate better self-awareness which will help them be able to bounce back more efficiently. Cognitive Behavioral Therapy (CBT) provides a tool for the work of creating better and clearer stories about facts that reduce negative bias (Beck, 1979; Ellis & Ellis, 2011; Reivich & Shatté, 2002). Even outside of clinical populations, CBT offers support to those struggling to deal with a fast-changing world by helping people to break down their thoughts and examine them (Reivich & Shatté, 2002). CBT rests on the theory that people can be trained to become aware of the content and process of their thoughts, that their interpretations of their thoughts can influence their emotions and behavior, and that individuals can modify these thought patterns to become more adaptable to the adversities that they face (Beck & Dozois, 2011).

Imagine an Information Systems Security Manager (ISSM) has received a report by an Information Systems Security Officer (ISSO) about a network security scan discrepancy. The ISSM, however, decides to focus on what they perceive as a different, more urgent and neglected issue and does not respond to the ISSO. Every day, ISSMs across the government have to decide how to use their limited time. Though ideally the ISSM should be responding to all reports from the ISSO to help manage risk to the system and direct incident response support, it is not always feasible to do so - particularly given the resource constraints and workload challenges mentioned earlier. If the ISSM found the next morning that the system that was the subject of the ISSO's report had been compromised, the ISSM might then start to worry about what else she may have neglected, how it may lead to the whole organization becoming compromised, and about the risk

that she might lose their job. The ISSM might then start to frantically review other unanswered reports and braces herself for a call from her manager.

Whether or not the ISSM's thoughts are real, none of those thoughts or actions helped to resolve the immediate issue at hand—the compromised system. Training cybersecurity professionals to deal with their thoughts will help them focus on preventing and solving problems. The adversity, thought, & consequence (ATC) model is a tool of self-awareness that help in this regard. In brief, the three components of the ATC model (figure 1) are: adversity, thoughts, and consequences (Ellis & Ellis, 2011; Reivich & Shatté, 2002). ATC is used to help understand what triggers ways of thinking that lead us to take actions that are not productive. When we become more comfortable examining our thoughts, our thoughts become easier to adjust.

| **Adversity** | **Thoughts** | **Consequences** |
|---|---|---|
| Compromised system | Believing that they will lose their job, and that the whole agency's network is compromised, as well as the other possible important things that have been forgotten | More time spent worrying than responding to the compromised system |

*Figure 1*. Adversity-Thoughts-Consequences (ATC). Adapted from "Cognitive Therapy And The Emotional Disorders" A. Beck, 1979.; "Rational Emotive Behavior Therapy" by A. Ellis & D. J. Ellis, 2011.

In this example, The ISSM was demonstrating some habits of mind that could cause undue emotional stress and slow her down from carrying out important tasks as well as. By viewing the ISSM's thoughts through the ATC model, it is easy to see how these thoughts derailed her from her tasks. Habits of mind are hard to change, even when people are open to revising their thoughts, because of cognitive errors. Research from the past few decades in

neuroscience and behavioral economics shows that people frequently make cognitive errors (Kahneman & Tversky, 1996). People make many decisions out of habit or intuition, which Kahneman (2011) describes as System 1 thinking. Slow methodological thought is considered System 2, but it is still not free from bias (Kahneman, 2011; Tversky & Kahneman, 1974).

Simply put, even if the ISSM was able to slow down in the moment and gain some self-awareness to focus on the task at hand, it is still may be hard for her to change her thinking pattern. Confirmation bias describes one's default reaction to look for information that validates what one already believes (good or bad; Nickerson,1998; Kahneman, 2011). Since this is a feature of human thinking, confirmation bias is found in all decision-making processes (whether System 1 or 2), and no one is immune to it (Kahneman, 2011). Although it is hard to change our minds because of the way our brains work, it is possible to do so. In this example, the ISSM can use the ATC method to notice their thinking patterns and begin to shift those patterns.

ATC can help the ISSM to notice patterns of thinking that bog her down, but it is only a partial step. Labeling the thinking pattern also helps to shift one's thoughts. Burns (1999) created a list (Figure 2) of what are considered to be common thinking traps. Through reviewing the list of thinking traps and comparing them to the ISSM's thinking, the ISSM could gain control of the pattern by labeling it, which increases her self-awareness (Southwick, 2012).

After reviewing the list, the ISSM would be able to label her thoughts as falling into thinking traps such as "jumping to a conclusion." Having the label helps to give the ISSM some emotional distance and control over her thoughts (Burns, 1999; Reivich & Shatté, 2002). "Jumping to conclusions" is a common thinking trap of taking small amounts of information and assuming the worst possible results. As the ISSM starts to notice she is "jumping to conclusions", for example, she can start to look for alternative explanations or wait for more

information. As noted with confirmation bias, it is hard to look for alternatives to our preconceived notions, but if the ISSM allows themselves to have curiosity about their thoughts, they reduce the tension of trying to validate their worst-case scenarios.

| **Thinking Trap** | **What it looks like?** |
|---|---|
| All-or-Nothing Thinking | Not seeing any nuance; Binary solutions |
| Over generalization | "Always" and "never" statements |
| Mental Filter | Focus on one event and see everything as related to it |
| Discounting the Positive | Attributing hard work to luck or that your best wasn't good enough |
| Jumping to Conclusions | Without evidence asserting something is true |
| Mind Reading | Claiming you knowing someone's internal motivations and thoughts |
| Magnification | Failing to see problems in context and minimizing your characteristics |
| Emotional Reasoning | You attribute your emotions to being factual reality instead of a complex web of information |
| Should statements | Words that indicate obligation, duty, or singular correct method exist...when no obligation, duty, or singular correct method exists |
| Labeling | Stating that your actions are your identity |
| Personalization and blame | You are singularly responsible for an action that has complex inputs that aren't under your control or stating that someone else is singularly responsible. |

*Figure 2*. Common Thinking Traps. Adapted from "The Feeling Good Handbook" by D. D. Burns, 1999.

Just as we can challenge our notions of the past, we can find a new reason for possible futures by cultivating optimism (Seligman, 1991). Our beliefs about the permanence, pervasiveness, personal reasons (good and bad) things happen are of great import and impact on our well-being (Peterson et al., 1982). An optimistic explanatory style has been shown to correlate with decreased signs of depressive symptoms (Peterson et al., 1982). Changing one's "explanatory style" is another tool the ISSM can use, which helps to move people from stories of uncontrollable tragedy to stories where goodness prevails (Seligman, 1991). For example, the ISSM can change her perspective on the situation she is wrestling with from a point of view that is pessimistic to one that is more optimistic. The ISSM can develop such an optimistic explanatory style by building an optimistic triad of thoughts. The optimistic triad asserts that good things are permanent, pervasive, and attributable to personal action (Seligman, 1991). The permanence of goodness helps to challenge thoughts about adverse circumstances becoming defining features of life. Focusing thoughts on the pervasiveness of goodness helps one to see that good things are happening all the time, and that adverse events are specific and temporal. Attributing the good things that happen in one's life to one's actions and bad things happening by chance increases our feelings of control over the world.

Let us reimagine the previous story. An Information Systems Security Manager (ISSM) has received a report by an Information Systems Security Officer (ISSO) about a possible security issue that may impact the authority to operate of the ISSO's system. The ISSM has to deal with a more urgent issue and neglects to respond to the ISSO. The next morning, the Security Operations Center reports that that system was compromised and that the incident response team is responding to the situation. The ISSM then starts to think about what else she may have forgotten, how this may lead to whole organization becoming compromised, and about

the risk that they might lose their job. The ISSM realizes that she may be "jumping to conclusions" and that she needs to focus on taking actions to secure the system instead. The ISSM reminds herself of her good fortune to work in an organization where she gets to use their skills and abilities, how she is surrounded by capable and competent people that will do the right thing to limit damage due to the compromised system, and that she has all of the training and authority they need to get the job done. The ISSM starts to contact her manager and alerts other parties to take immediate actions.

**Relationships that work.**

"Will you be there for me?" - that is the fundamental question that most relationships rest on (Gable, Gonzaga, & Strachman, 2006). How people treat those around them determines the quality of their connections (Dutton, 2003), and how they respond to their partners in daily events is a determinate of the health and length of a relationship (Drivers & Gottman, 2004). Capitalizing is spending time sharing and savoring positive events with others; this process increases the positive emotions of both listener and speaker (Reis et al., 2010). Savoring positive events helps people magnify their enjoyment of the event. Positive emotions help to build the internal resources to face challenges and opens our minds to other opportunities (Frederickson, 2001). Capitalizing increases relationship health more than merely being supportive in bad times (Gable et al., 2006).

Nevertheless, as shown in Figure 3, it is easy to see how a cybersecurity professional could throw such an opportunity away through passive constructive responses (PCR, showing obvious disinterest), passive destructive response (PDR, failing to engage with the moment), and active destructive response (ADR, being openly hostile to the moment, Gable et al., 2006; Reis et al., 2010). A person can simply acknowledge that he heard the person without seeking further

information (PCR) as is the case in the example, or he can ignore the story someone is telling him (PDR). A person can also devalue the story by pointing out the flaws in the other person's logic or by changing the topic (ADR). These methods not only reduce a partner's or colleagues joy but also diminishes his relationship to the listener.

| | **Constructive** | **Destructive** |
|---|---|---|
| **Active** | What happened next?<br><br>How did you feel?<br><br>Where were you when you found out?<br><br>I'm so happy for you! Do you have time to tell me more? Details! | Wow! They didn't include you with team that went to trial!<br><br>Are you sure it is the same case?<br><br>Do you have a plan for how you can be a part of a great team like that one?<br><br>I can't believe that they actually won. |
| **Passive** | That is good for you.<br><br>That's great news.<br><br>Terrific.<br><br>Congratulations. | I have to tell you about what just happened to me.<br><br>Did you hear about the good news that happened to another friend?<br><br>That's similar to what happened to me a couple of years ago. |

*Figure 3*. Active Constructive Response (ACR) Model. Adapted from "Will You Be There For Me When Things Go Right? Supportive Responses To Positive Event Disclosures" by S. L. Gable, G. C. Gonzaga, & A. Strachman, *Journal of Personality and Social Psychology,* 2006, p. 905-906.

Cybersecurity professionals may miss the opportunity to capitalize with colleagues when they don't focus on their interaction in the present moment. There can be a lot of good things happening every day when cyber security professionals are at work but there are a lot of challenges competing for one's attention. Capitalizing depends on being mindfully present with others and responding to them in a meaningful way. To illustrate the point, here is a conversation

between a digital forensics analyst (DF) and their manager (MG). The DF was a part of a large team that supported the prosecution of a hacker group that attacked JP Morgan.

DF: I saw on the news that the JP Morgan data breach case I worked on a few years ago ended with a conviction.

MG: That's great news.

DF: I worked so hard to get the analysis right and worked with a great team of experts.

MG: I know. I am really glad it all worked out.

DF: Me too.

Here we see a typical conversation between colleagues. There is it anything inappropriate about the MG's response. However, there are ways to take exchanges like the one above and transform them into relationship building moments. Changing the way the MG responds to the good news of the DF can make a vital difference.

The primary method of capitalization is an active constructive response (ACR, Gable et al., 2006). ACR focuses on how and why something has been positive for someone else with a sense of curiosity. Being able to use ACR in a way that deepens the partner's experience of telling the events calls for emotional granularity. Emotional granularity is finding the precise words to describe an emotional experience (Smidt & Suvak, 2015). People who use emotionally granular language in describing their bad experiences have less distress when recounting bad moments (Smidt & Suvak, 2015). There is evidence that suggests this might also enhance positive experiences as well (Smidt & Suvak, 2015). Let us revisit the past conversation to see how it would work.

DF: I saw on the news that the JP Morgan data breach case I worked on a few years ago ended with a conviction.

MG: Where were you when you found out?

DF: I was sitting at my desk and saw it flash on the news. I was very surprised.

MG: How did you feel?

DF: I was in shock and very excited.

MG: What was the most shocking part? Was it more completely astonishing, exhilarating, or something else?

DF: Good question. Come to think of it was more like astonishing. I had totally put that work out of my mind. I haven't thought about it in a year or so. It feels good to be part of something that made a difference.

MG: Sounds like you were part of a great team. You all did amazing work. I would love to hear more later.

DF: Thank you! I have to finish up some projects this week, but I can swing by your office next week.

MG: Sounds like a plan.

The differences between the conversations are clear. Using ACR would deepen the DF's experience as well as opens the door for further conversation. ACR is a pathway to build and sustain relationships. It is a tool that should be used wisely and has great promise. Capitalizing on the good that comes into the lives of the people we work with or just the people that happen to be around is a worthwhile effort. Getting to know precisely what makes this moment beautiful for others, through emotionally granular language, may lead to gratitude for the goodness that surrounds them (Gable et al., 2006; Smidt & Suvak, 2015).

## Psychological Safety

Positive institutions create thriving individuals and psychological safety is a strategy they can employ to help do so (Seligman & Csikszentmihalyi, 2000; Edmonson, 1996). Psychological safety comes from being in an environment where people can fully be themselves and express their thoughts (Edmonson, 1996). Cybersecurity professionals need to be able to work in such open workplaces. The tasks that they perform are across a wide range of subjects and specialties, but the common thread is that teamwork is antecedent to success (Parker, Winslow, & Tetrick, 2016). Psychological safety is an outcome from trust and respect across people working together, which increase feelings of well-being by improving the quality of relationships between people in the organization (Carmeli & Gittell, 2009; Edmonson, 1996). This section will cover the need to be comfortable reporting failures, voicing dissent, increasing performance, and cultivating psychological safety.

### Reporting Failures.

Researchers have found that when there is trust and respect among team members, reports of errors goes up, and that is due to their feeling free to discuss failures (Edmondson, 1996). Continued growth and development are essential elements of a cybersecurity workforce. (Dawson & Thomson, 2018) and learning often takes places by understanding such errors (Edmondson, 2019). Cybersecurity professionals not only need to know what to do but also how to do it. This how-to type of knowledge often comes from working in coordination with teams (Tucker, Nembhard, & Edmondson, 2007). And technically proficient cybersecurity professionals will be more effective if they can learn from one another.

Learning from failure is key to sustaining proficiency. If there is a culture of denying failures, then errors will go unreported (Tucker & Edmondson, 2003). Unreported errors will

inevitably cause harm to the government and the general public. What is more, cybersecurity professionals might start to rely on workarounds to do routine work, slowing down the ability to react to emerging issues. Workarounds are a sign of lack of psychological safety (Halbesleben & Rathert, 2008). Cybersecurity professionals need to have processes in place that work and need to be able to speak up to make sure that these processes are working.

Let's revisit the story of the ISSM missing an important report from an ISSO. The ISSM's thoughts were geared toward personal failure, possibly because the environment was primed for that response. In an environment where errors are openly discussed, the ISSM would know that she could own her role in the incident and be treated fairly. She would know that she could start to take actions to continue to support the incident response. Of course, that wouldn't eliminate her ingrained thought patterns, but a psychologically safe environment would provide support to report her mistakes instead of sitting in silence.

**Breaking the Silence.**

If cybersecurity professionals don't feel that they can speak up and share their knowledge won't be passed on. The technical skills that are needed for various roles in cybersecurity vary by a wide margin, but the common thread is teamwork (Jose, LaPort, & Trippe, 2016). A team will not function if teammates can't learn from each other. Learning comes often by feeling that your voice matters (Detert & Edmondson, 2011). Implicit voice theories are the unspoken beliefs about when it is appropriate to speak up at work (Deter & Edmondson, 2011). Cybersecurity professionals will make decisions based on what they perceive is the benefit of speaking (figure 4; Detert & Edmondson, 2011). These implicit voice theories start to stifle communication because the perceived cost of voicing their thoughts is higher than the perceived benefit. Organizations lose out on valuable insights, teams lack candor,

and employees feel unheard when these implicit voice theories weigh heavily against speaking up.

| | **Who Benefits** | **When Benefits Occurs** | **Certainty of Benefit** |
|---|---|---|---|
| **Voice** | The organization and/or the public | After some delay | Low |
| **Silence** | Oneself | Immediately | High |

*Figure 4*. Why Silence Wins in the Voice Silence Calculation. From "The Fearless Organization" by A. Edmonson, 2019, p. 34.

Recall, the PM using their character strength of curiosity at work. Curiosity can come in many forms from becoming very introspective about your own inner workings to wanting to discover more about how to improve our work environment (Niemic, 2018). A PM using their character strength, curiosity will start to ask a lot of questions of their peers, subordinates, and superiors. In an environment where the implicit voice calculation is weighed against speaking up, the curious PM will find that they could be marginalized and distrusted by violating this unspoken norm.

Ensuring that cybersecurity professionals weigh toward voicing their concerns and sharing knowledge with their teammates is imperative to create psychological safety (Siemsen, Roth, Balasubramanian, & Anand, 2009). Creating environments where cybersecurity professionals see it is normal to speak about disagreements, errors, and process improvements will benefit the organization (Parker, Winslow, & Tetrick, 2016). Not only will it be hard to solve problems, but having cybersecurity professionals feel inhibited from speaking is hard to have an exchange of ideas that can create new possibilities (Parker, Winslow, & Tetrick, 2016). The free exchange of ideas is necessary in knowledge-based roles such as cybersecurity.

**Increasing Performance.**

Psychological safety matters for performance as demonstrated by Google's Project Aristotle. Project Aristotle is how Google sought to understand teams better. Through reviewing hundreds of teams to see what the common variables are, the only one thing that was in common was psychological safety (Duhigg, 2016). Teams that were composed of diverse viewpoints and skill levels did better than teams that were all top performers, but didn't have psychological safety in their group (Duhigg, 2016). The essential element in teams is not to have a "work face;" they want real people that are going to be alongside them as they work toward their goals (Duhigg, 2016). The highest performing teams aren't the teams with the best credentials - they are the teams that work the best together (Edmonson, 2003).

In Taiwan, a study examined 60 teams that included 245 people and found that teams with psychological safety had the best performance metrics (Huang & Jiang, 2012). The lack of fear of embarrassment for expressing ideas was seen as essential to increasing team performance (Huang & Jiang, 2012). These teams focused on R&D that is particularly geared toward the generation of new ideas. Knowledge work requires teams to be ready to share without hesitation what they see and come to a new understanding. Psychological safety is needed to ensure that sharing occurs.

As a case in point, imagine how experience of a digital forensics analyst (DF) and his manager (MG) discussing their role in the case of the JP Morgan data breach, as presented earlier, illustrates how a conversation could be a catalyst for deeper understanding that could increase the current team's performance. Having someone that worked first-hand on such a prominent case is invaluable. The DF likely has a lot of both practical knowledge and technical knowledge to share about how his previous team was successful. The way that the MG interacts

with the DF could encourage the DF to teach others or to remain silent. An environment of psychological safety makes it possible to share information with others without fear.

**Much to Fear, Ways to be Fearless**

The world that cybersecurity professionals inhabit (described earlier as VUCA) both in their organizational settings and the larger world that they face (Stiehm, 2002). There are challenges from many areas in how they are able to accomplish their duties. However, as described earlier, there are many ways that a cybersecurity professional can thrive in a VUCA world. Ensuring that cybersecurity professionals have psychological safety—an environment that brings the best out of them as individuals and teams—is the primary way to thrive in a VUCA world.

The antecedents of a psychologically safe environment look similar to what has been discussed earlier in supporting PERMA and building resilience that also help people thrive in uncertainty. Creating positive emotions such as trust and curiosity are key components to building psychological safety (Delizonna et al., 2017). Trust has to be built through deliberate action such as reframing failure (Tucker, Nembhard, & Edmondson, 2007). In psychologically safe environments, failure is looked at as part of learning; in this context, it is differentiated from mistakes that happened from violating a law or procedure (Edmonson, 2019).

Everyone from leaders to front-line workers owns a part of maintaining psychological safety. Leaders must demonstrate that they care about learning and not about blame and set-up procedures where errors are reviewed, so that the team can learn from each other. In some organizations, this will look like a formal review of events; in other organizations, this review process may take the form of short weekly roundtable discussions about what didn't go well and

why. Yet, no matter the form it takes, the review process should be a learning tool, not a weapon to punish or humiliate (Edmonson, 2003).

Learning helps to transform the workplace to one in search of problems, to one in search of opportunities. It is necessary to strike a balance of having high standards and high psychological safety (Figure 5, Edmonson, 2019). Keeping employees at the peak of learning and performance is critical without having employees drift into their comfort zone. High standards and high psychological safety yield high performance. Psychological safety isn't about being nice, but allowing people permission to be human.

| | **Low Standards** | **High Standards** |
|---|---|---|
| **High Psychological Safety** | Comfort Zone | Learning & High Performance Zone |
| **Low Psychological Safety** | Apathy Zone | Anxiety Zone |

*Figure 5*. Performance and Psychological Safety. From "The Fearless Organization" by A. Edmonson, 2019, p. 18.

It is hard to cultivate psychological safety in leadership cultures that insist on blame and control as a primary tool motivate performance (Carmeli & Gittell, 2009). Psychological safety calls for everyone on the team to act with trust and respect. However, it is hard to move away from ingrained notions about blame and control. A new idea of what failure is should be accepted by the team—failure as learning. Edmonson (2019) describes this as "setting the stage" (figure 6).

| | **Setting the Stage** | **Inviting Participation** | **Responding Productively** |
|---|---|---|---|
| **Leadership** | **Frame the Work**<br><br>• Set expectations about failure, uncertainty, and interdependence to clarify the need for voice<br><br>**Emphasize Purpose**<br><br>• Identify what's at stake, why it matters, and for whom it matters | **Demonstrate Situational Humility**<br><br>• Acknowledge gaps<br><br>Practice Inquiry<br>• Ask good questions<br>• Model intense listening<br><br>**Set Up Structures and Processes**<br><br>• Create forums for input<br>• Provide guidelines for discussion | **Express Appreciation**<br><br>• Listen<br>• Acknowledge and thank<br><br>**Destigmatize Failure**<br><br>• Look forward<br>• Offer help<br>• Discuss, consider, and brainstorm next steps<br><br>**Sanction Clear Violations** |
| **Accomplishes** | Shared expectations and meaning | Confidence that voice is welcome | Orientation toward continuous learning |

*Figure 6*. The Leaders Toolkit. From "The Fearless Organization" by A. Edmonson, 2019, p. 159.

**Ways to Cultivate Psychological Safety**

Leaders must model what it looks like to fail well because there is a deep fear of losses (Kahneman & Tversky, 1979; Kahneman, 2011; Tucker, Nembhard, & Edmondson, 2007). When people feel that the cost of trust is too high, they simply won't trust (Shallcross & Simpson, 2012). Lowering the cost of trust can happen by leaders demonstrating the behavior that they seek from the team. Edmonson (2019) describes this as inviting participation.

Inviting participation means leaders need to have a structured way to have discussions as and be able to listen closely to feedback (Hirak, Peng, Carmeli, & Schaubroeck, 2012). The team must know that all voices are valued and that their ideas are welcomed. The structure that will vary depending on whether the cybersecurity professionals work on a watch floor, lab, or traditional office setting. However, the key is for leaders to develop forums for open exchange of ideas that protect the dignity of the workforce. Leaders must also be open to being questioned and be comfortable asking questions that help create a thriving learning environment. Imagine, at a project meeting, an IT project manager sought the feedback of the team on why the schedule has slipped with questions that are focused on understanding, not assigning blame (Delizonna et al., 2017). In that type of environment, there is robust discussion and solutions are found. All the team members would know that their voices aren't merely being tolerated, but their voices are welcome.

In order to make everyone feel welcomed, everyone must respond productively to questions and comments. Appreciation is at the heart of starting a conversation to maintain psychological safety (Nembhard & Edmondson, 2006). How appreciation is expressed helps to demonstrate that someone can voice their authenticity, no matter the quality (Edmonson, 2019). By acknowledging all voices, it becomes easier for others to speak up especially if there is a difference in the status of the participants (Kahn, 1990). Also, when voices that speak of failure are met with problem solving and other types of assistance, it makes it easier to bring up issues to the team. Failure soon becomes part of the learning of the team and builds everyone's capability (Hirak, Peng, Carmeli, & Schaubroeck, 2012).

The practices highlighted in this section can help shift the cybersecurity work environment to one that fosters psychological safety. Cybersecurity professionals' work is often not routine and unpredictable, so encouraging learning throughout the organization is essential. Greater openness to a free exchange of ideas will help cybersecurity professionals grow enable them to do their job effectively. And doing so does not have to get in the way of appropriately adhering to necessary ethical, procedurals, and legal standards that are critical to a cybersecurity professional's work. Creating psychological safety in the public sector work environments of cybersecurity professionals may yield results that have been seen at places like Google, where employees thrive because the culture allows it, and their organization excels as a result.

## Training and Testing

Resilience skills and psychological safety form the bedrock of what cybersecurity professionals need to thrive. Resilience training has been offered in various forms by many different organizations. Building psychological safety, as seen in this paper, is also a trainable skill. Determining what type of resilience and psychological safety training will be dependent on what protective factors an organization wants to enhance. However, to determine if the training is effective, it will need testing. As an example, Appendix B gives a possible experimental design to test the effectiveness of resilience and psychological safety training program focused on cybersecurity professionals, which will happen by the following three recommendations:

1) Train cybersecurity professionals with resilience skills in a program similar to ones used by the US Air Force, US Navy, or US Army's Master Resilience Training (MRT). In particular, the US Army's MRT has been shown to increase individual's self-reports of well-being and have reduced reports of behavioral health problems (Griffith & West,

2013). Other agencies, such as, the Department of Homeland Security are also investing in developing resiliency programs.

2) Have cybersecurity professionals identify their character strengths using the VIA survey and discuss the results to create space for cybersecurity professionals to use their character strengths at work (Niemic, 2018).

3) Provide managers and supervisors training on facilitating psychological safety in the workplace (Google, n.d.).

4) Monitor the effectiveness of these strategies through agency-wide surveys that measure well-being, psychological safety, and resilience

Cybersecurity professionals that have been trained to be more self-aware, build better relationships, use their character strengths, become more optimistic, develop mental agility, and self-regulate are going to have the edge over the adversaries that they will face. All of these elements help to build resilience. Creating resilience in the cybersecurity workforce could lead to better retention. Retention of cybersecurity professionals have narrowly focused on compensation and speed of hiring (Serbu, 2019). However, resilience training provides another method to support and retain cybersecurity professionals.

Monitoring the progress of resilience and psychological safety training through using validated tools such as the PERMA-profiler, Positive, Negative Affect Schedule (PANAS) and Edmonson 7-item survey (Butler & Kerns, 2016; Crawford & Henry, 2004; Edmonson, 1999). This will help to ensure that these efforts stay on track. Although these concepts have been implemented elsewhere, being able to draw from data that accounts from individual agencies will help determine if the predicted improvements happen. Monitoring progress also signals to all levels of the organization that the program is serious about addressing employee well-being. If

the programs to train cybersecurity professionals in resilience and psychological safety skills are not effective, the programs should stop.

**Towards a Positive Public Service for Cybersecurity Professionals**

This paper sought to explain how positive experiences, positive traits, resilience and psychological safety can enhance cybersecurity professionals' well-being. Positive experience as described by PERMA help to highlight the ways individuals can take control of their well-being. Positive traits (character strengths) can bring the best out of cybersecurity professionals and those around them. Resilience skill building can increase the effectiveness of cybersecurity professionals and improve their well-being. When cybersecurity professionals know that they are in an environment where they are trusted and respected, they perform at their best. Psychological safety is present when people can report failures, speak up authentically, and receive support to be their best self. Cybersecurity professionals need that type of environment to perform their complex and varied work. To help develop that kind of an environment for cybersecurity professionals, leaders must set the stage by helping everyone understand the purpose of their work, invite participation to create new ideas and challenge old beliefs, and respond productively by not shaming failure.

Training is just the beginning of the path toward building positive institutions to support cybersecurity professionals in the federal government. The descriptions discussed help to outline a "positive public service" (Jones, 2017, p. 57) for cybersecurity professionals that focuses on turning government institutions that are doing great work for the country into places of thriving for their workers. Cybersecurity professionals are doing many things right, and cybersecurity professionals have an opportunity to make what is right even better. Cybersecurity professionals that have both the technical competency and professionals skills to be productive in a VUCA

world is a necessity, but they also need tools to thrive in the face of the adversity. Positive experiences and traits as well as resilience and psychological safety are ingredients to fuel their future success.

References

Bonanno, G. A. (2012). Uses and abuses of the resilience construct: Loss, trauma, and health-related adversities. *Social Science & Medicine, 74*(5), 753-756.

Beck A. T. (1979). *Cognitive therapy and the emotional disorders*. United States: Meridian Book.

Beck, A. T., & Dozois, D. J. (2011). Cognitive therapy: current status and future directions. *Annual Review of Medicine*, *62*, 397-409.

Burns, D. D. (1999). *The feeling good handbook* (Rev. ed.). New York, N.Y., U.S.A.: Plume.

Butler, J., & Kern, M. L. (2016). The PERMA-profiler: A brief multidimensional measure of flourishing. *International Journal of Wellbeing, 6*(3), 1-48.

Buhler, C. (1971). Basic theoretical concepts of humanistic psychology. *American Psychologist, 26(4)*, 378-386.

Cameron, K. S., Dutton, J. E., & Quinn, R. E. (Eds.). (2003). *Positive organizational scholarship*. San Francisco, CA: Berrett-Koehler.

Carmeli, A., & Gittell, J. H. (2009). High-quality relationships, psychological safety, and learning from failures in work organizations. *Journal of Organizational Behavior, 30*(6), 709-729.

Crawford, J. R., & Henry, J. D. (2004). The positive and negative affect schedule (PANAS): Construct validity, measurement properties and normative data in a large non-clinical sample. *British Journal of Clinical Psychology, 43*(3), 245-265.

Csikszentmihalyi, M. (1990). *Flow: the psychology of optimal experience*. New York, NY: Harper Perennial.

Davis, W. E., Kelley, N. J., Kim, J., Tang, D., & Hicks, J. A. (2016). Motivating the academic mind: High-level construal of academic goals enhances goal meaningfulness, motivation, and self-concordance. *Motivation and Emotion*, *40*(2), 193-202.

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology, 9*, 744.

Delizonna, L., Tjan, A. K., Walker, C. A., D'Souza, S., & Renner, D. (2017, August 24). High-Performing Teams Need Psychological Safety. Here's How to Create It. Retrieved from https://hbr.org/2017/08/high-performing-teams-need-psychological-safety-heres-how-to-create-it

Detert, J. R., & Edmondson, A. C. (2011). Implicit voice theories. *Academy of Management Journal, 54*(3), 461-488.

Diener, Ed (1984). Subjective well-being. *Psychological Bulletin*, *95*(3), 542–575.

Driver, J. & Gottman, J. (2004). Daily marital interactions and positive affect during marital conflict among newlywed couples. *Family Process,43*(3), 301-314.

Duckworth, A. (2016). *Grit: the power of passion and perseverance*. New York, NY: Scribner.

Duckworth, A., Steen, T. A., & Seligman, M. E. P. (2005). Positive psychology in clinical practice. *Annual Review of Clinical Psychology*, *1*(1), 629-651.

Duckworth, A., Peterson, C., Matthews, M. D., & Kelly, D. R. (2007). Grit: Perseverance and passion for long-term goals. *Journal of Personality and Social Psychology*, 92, 1087-1101.

Duffy, R. D., Diemer, M. A., Blustein, D. L., & Autin, K. L. (2016). The psychology of working theory. *Journal of Counseling Psychology, 63*(2), 127-148.

Duhigg, C. (2016, Feb 25,). What google learned from its quest to build the perfect team. *New*

*York Times (Online),* Retrieved from https://search.proquest.com/docview/1768006775

Dutton, J. E. (2003). *Energizing your workplace: Building and sustaining high quality relationships at work.* San Francisco: Jossey J. Bass.

Edmondson, A. C. (1996). Learning from mistakes is easier said than done: Group and organizational influences on the detection and correction of human error. *Journal of Applied Behavioral Science, 32*(1), 5-28.

Edmondson, A. C. (2003). Managing the risk of learning: Psychological safety in work teams. In M. A. West, K. G. Smith, & D. Tjosvold (Eds.) *International handbook of organizational teamwork and cooperative working* (pp. 255-275). Chichester, UK: John Wiley & Sons Ltd.

Edmondson, A. C. (2019) *The fearless organization: Creating psychological safety in the workplace for learning, innovation, and growth*. Hoboken, NJ: John Wiley & Sons.

Edmondson, A. C., & Lei, Z. (2014). Psychological safety: The history, renaissance, and future of an interpersonal construct. *Annual Review of Organizational Psychology and Organizational Behavior, 1*(1), 23-43.

Ellis, A., & Ellis, D. J. (2011). *Rational emotive behavior therapy*. Washington, DC: American Psychological Association.

Executive Order No. 13870, 3 C.F.R. 20523 - 20527 (2019).

Farmer, C. M., Whipkey, K., & Chamberlin, M. (2019, March 26). Programs addressing psychological health and resilience in the U.S. Department of Homeland Security. Retrieved from https://www.rand.org/pubs/research_reports/RR1952.html

Feder, A., Haglund, M., Wu, G., Southwick, S. M., & Charney, D. S. (2013). The neurobiology of resilience. In D. S. Charney, J. D. Buxbaum, P. Sklar, & E. J. Nestler

(Eds.), *Neurobiology of mental illness* (pp. 1144-1170). New York, NY, US: Oxford University Press.

Federal Acquisition Regulation (FAR), 48 C.F.R. (2019).

Frankl, V. E. (1992). *Man's search for meaning: An introduction to logotherapy* (4th ed.) (I. Lasch, Trans.). Boston, MA, US: Beacon Press.

Frederickson, B. L. (2001). The role of positive emotions in positive psychology: The broaden-and-build theory of positive emotions. *American Psychologist, 56*(3), 218-226.

Fredrickson, B. L. (2013). Updated thinking on positivity ratios. *American Psychologist, 68*(9), 814-822.

Freidlan, P., Littman-Ovadia, H., & Niemiec, R., M. (2017). Positive psychopathology: Social anxiety via character strengths underuse and overuse. *Personality and Individual Differences, 108,* 50-54.

Fruhlinger, J. (2018, August 30). What is WannaCry ransomware, how does it infect, and who was responsible? Retrieved from https://www.csoonline.com/article/3227906/what-is - wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

Gable, S. L., Gonzaga, G. C., & Strachman, A. (2006). Will you be there for me when things go right? Supportive responses to positive event disclosures. *Journal of Personality and Social Psychology, 91*(5), 904-917.

Giles, M. (2018, August 20). Cybersecurity's insidious new threat: Workforce stress. Retrieved From https://www.technologyreview.com/s/611727/cybersecuritys-insidious-new-threat-workforce-stress/

Gibson, D. (2015). *Managing Risk in Information Systems;* (2nd ed.). Burlington, MA:

Jones and Bartlett Learning.

Google. (n.d.). Re:Work - Guide: Understand team effectiveness. Retrieved from https://rework.withgoogle.com/guides/understanding-team-effectiveness/steps/foster-psychological-safety/

Grant, A. M., & Schwartz, B. (2011). Too much of a good thing: The challenge and opportunity of the inverted U. *Perspectives on Psychological Science*, *6*(1), 61–76.

Griffith, J., & West, C. (2013). Master resilience training and its relationship to individual well-being and stress buffering among army national guard soldiers. *The Journal of Behavioral Health Services & Research, 40*(2), 140-155. doi:10.1007/s11414-013-9320-8

Halbesleben, J., & Rathert, C. (2008). The role of continuous quality improvement and psychological safety in predicting work-arounds. *Health Care Management Review.*, *33*(2), 134–144.

Hirak, R., Peng, A. C., Carmeli, A., & Schaubroeck, J. M. (2012). Linking leader inclusiveness to work unit performance: The importance of psychological safety and learning from failures. *The Leadership Quarterly, 23*(1), 107-117.

Howell, R. T., Kern, M. L., & Lyubomirsky, S. (2007). Health benefits: Meta-analytically determining the impact of well-being on objective health outcomes. *Health Psychology Review, 1*(1), 83-136.

Horowitz, D. (2018). *Happier?*. New York, NY: Oxford University Press.

Hsieh, C (2018). No one can serve two masters: Revisiting the interaction effect of love of money and public service motivation on job satisfaction. *Public Performance & Management Review*, *41*(4), 745–767.

Huang, C., & Jiang, P. (2012). Exploring the psychological safety of R&D teams: An empirical

analysis in Taiwan. *Journal of Management & Organization, 18*(2), 175-192.

Jones, B.J. (2017). *Positive public service: Turning purpose into progress by changing how government works from the inside. (*Unpublished master's capstone). University of Pennsylvania, Philadelphia, Pennsylvania.

Jose, I., LaPort, K., & Trippe, D. M. (2016). Requisite attributes for cyber security personnel and teams: Cyber risk mitigation through talent management. In S. J. Zaccaro, R. S. Dalal, L. E. Tetrick, & J. A. Steinke (Eds.), *Series in applied psychology. Psychosocial dynamics of cyber security* (pp. 167-193). New York, NY, US: Routledge/Taylor & Francis Group.

Kahn, W. A. (1990). Psychological conditions of personal engagement and disengagement at work. *Academy of Management Journal*, *33*, 692–724

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica, 47*, 263-291.

Kahneman, D., & Egan, P. (2011). *Thinking, fast and slow* (Vol. 1). New York: Farrar, Straus and Giroux.

Kahneman, D., & Tversky, A. (1996). On the reality of cognitive illusions. *Psychological Review*, *103*(3), 582-591.

Klimoski, R., Murray, J. (2016) Cyber security executive leadership. In S. J. Zaccaro, R. S. Dalal, L.E. Tetrick, & J.A. Steinke, (Eds.), *The Psychosocial dynamics of cyber security*. New York: Taylor & Francis/Routledge.

Lee, M. (2019). Trump's cyber workforce order gets bipartisan praise. Retrieved from https://www.politico.com/newsletters/morning-cybersecurity/2019/05/03/trumps-cyber-workforce-order-gets-bipartisan-praise-608298

Luthans, F. (2002). Positive organizational behavior: Developing and managing psychological strengths. *Academy of Management Executive, 16*(1), 57–72.

Luthans, F., & Youssef, C. M. (2004). Human, social, and now positive psychological capital management: Investing in people for competitive advantage. *Organizational Dynamics, 33*, 143–160.

Lopez, S., Snyder, C., Masten, A., Cutuli, J., Herbers, J., & Reed, M. (2009). Resilience in Development. In C. R. Snyder & S. J. Lopez (Eds.) *The Oxford handbook of positive psychology* (2nd ed., pp. 589–598) New York, NY: Oxford University Press.

Martela, F., Martela, F., & Steger, M. F. (2016). The three meanings of meaning in life: Distinguishing coherence, purpose, and significance. *The Journal of Positive Psychology, 11*(5), 531-545.

Martínez-Martí, M. L., & Ruch, W. (2017). Character strengths predict resilience over and above positive affect, self-efficacy, optimism, social support, self-esteem, and life satisfaction. *The Journal of Positive Psychology*, *12*(2), 110-119.

Maslow, A. H. (1954). *Motivation and personality*. New York: Harper.

Masten, A. S. (2014). *Ordinary magic: Resilience in development*. New York, NY: Guilford Press.

Melchert, N. (2002). Aristotle: The reality of the world. The good life. In *The great conversation:A historical introduction to philosophy* (pp. 186-195). Boston, MA: McGraw- Hill.

Mowery, D. C., & Simcoe, T. (2002). Is the internet a US invention?—an economic and technological history of computer networking. *Research Policy, 31*(8), 1369-1387.

Nembhard, I. M., & Edmondson, A. C. (2006). Making it safe: The effects of leader

inclusiveness and professional status on psychological safety and improvement efforts in health care teams. *Journal of Organizational Behavior, 27*(7), 941-966.

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). *NIST Special Publication 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* (United States, Department of Commerce, National Institute of Standards and Technology). Gaithersburg, MD: National Institute of Standards and Technology.

Nickerson, R. S. (1998). Confirmation bias: A ubiquitous phenomenon in many guises. *Review of General Psychology*, *2*(2), 175-220.

Niemiec, R. (2018).*Character strengths interventions: A field guide for practitioners.* Hogrefe Publishing. Toronto, Canada.

Owens, B. P., Johnson, M. D., & Mitchell, T. R. (2013). Expressed humility in organizations: Implications for performance, teams, and leadership. *Organization Science*, *24*(5), 1517-1538.

Parker, S., Winslow, C.J. & Tetrick, L.T. (2016). Designing meaningful, healthy, and high performing work in cyber security. In S. J. Zaccaro, R. S. Dalal, L.E. Tetrick, & J.A. Steinke (Eds.), *The psychosocial dynamics of cyber security*. New York: Taylor & Francis/Routledge.

Peterson, C., Semmel, A., von Baeyer, C., Abramson, L. Y, Metalsky, G. I., & Seligman, M. E. P. (1982). The Attributional Style Questionnaire. *Cognitive Therapy and Research, 6,* 287-299.

Peterson C. & Seligman M.E. (2004). *Character strengths and virtues: A handbook and classification* (Vol. 1). Oxford University Press. New York, NY.

Peterson, C. (2006). *A primer in positive psychology*. Oxford: Oxford University Press. New

York, NY.

Perry, J. L., & Wise, L. R. (1990). The motivational bases of public service. *Public Administration Review, 50*(3), 367.

Prilleltensky, I., Dietz, S., Prilleltensky, O., Myers, N. D., Rubenstein, C. L., Jin, Y., & McMahon, A. (2015). Assessing multidimensional well-being: Development and validation of the i coppe scale. *Journal of Community Psychology, 43*(2), 199-226.

Reivich, K., & Shatté, A. (2002). *The resilience factor: 7 essential skills for overcoming life's inevitable obstacles*. New York, NY, US: Broadway Books.

Reivich, K. J., Seligman, M. E. P., & McBride, S. (2011). Master resilience training in the U.S. Army. *American Psychologist, 66*(1), 25-34.

Reis, H., Smith, S., Carmichael, C., Caprariello, P., Tsai, F., Rodrigues, A. & Maniaci, M.(2010). Are you happy for me? How sharing positive events with others provides personal and interpersonal benefits. *Journal of Personality and Social Psychology, 99(2)*, 311-329

Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist*, *55(1)*, 68–78.

Ryff, C. D. (1989). Happiness is everything, or is it? Explorations on the meaning of psychological well-being. *Journal of Personality and Social Psychology, 57*(6), 1069-1081.

Seligman, M. E. P. (1991). *Learned optimism: A leading expert on motivation demonstrates that optimism.* New York: Simon and Schuster.

Seligman, M. E. P. (2013). *Flourish: A visionary new understanding of happiness and well-being*. New York, NY: Atria.

Seligman, M. E. P., & Csikszentmihalyi, M. (2000). Positive psychology: An introduction.

*American Psychologist, 55*(1), 5-14.

Seligman, M. E. P. (2015). Chris peterson's unfinished masterwork: The real mental illnesses. *The Journal of Positive Psychology, 10*(1), 3-6.

Serbu, J. (2019, March 20). New DoD personnel system hires cyber workers faster but numbers small. Retrieved from https://federalnewsnetwork.com/dod-reporters-notebook-jared-\ serbu/2019/03/new-dod-personnel-system-hires-cyber-workers-faster-but-numbers-small/

Shallcross, S. L., & Simpson, J. A. (2012). Trust and responsiveness in strain-test situations: A dyadic perspective. *Journal of Personality and Social Psychology, 102*(5), 1031-1044

Smidt, K. E., & Suvak, M. K. (2015). A brief, but nuanced, review of emotional granularity and emotion differentiation research. *Current Opinion in Psychology, 3*, 48-51.

Smith, E. E. (2017). *The power of meaning: Crafting a life that matters*. New York, NY: Crown.

Southwick, S. M., & Charney, D. S. (2012). *Resilience: the science of mastering lifes greatest challenges*. Cambridge: Cambridge University Press.

Stiehm, J. (2002). *The US army war college: Military education in a democracy*. Philadelphia: Temple University Press.

Tay, L., Tan, K., Diener, E., & Gonzalez, E. (2012). Social relations, health behaviors, and health outcomes: A survey and synthesis. *Applied Psychology: Health and Well-being*, *5*(1), 28-78.

The White House. (2018, Dec 19). *Press briefing on the attribution of the wannacry malware attack to North Korea* [Interview transcript]. Retrieved from: https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/

Tucker, A. L., & Edmondson, A. C. (2003). Why hospitals don't learn from failures: Organizational and psychological dynamics that inhibit system change. *California Management Review, 45*(2), 55-72.

Tucker, A. L., Nembhard, I. M., & Edmondson, A. C. (2007). Implementing new practices: An empirical study of organizational learning in hospital intensive care units. *Management Science, 53*(6), 894-907.

Tversky, A.,& Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science*, *185*, 1124–1131.

World Health Organization. (2019, May 28). Burn-out an "occupational phenomenon": International Classification of Diseases. Retrieved from https://www.who.int/mental_health/evidence/burn-out/en/

Wrzesniewski, A., & Dutton, J.E. (2001). Crafting a job: Revisioning employees as active crafters of their work. *Academy of Management Review, 26*(2), 179-201

## Appendix A

| Activating Event | Thoughts | Consequences |
|---|---|---|
| | | |
| | | |
| | | |

*Figure 1*. Sample ATC Worksheet. Adapted from "Cognitive Therapy And The Emotional Disorders" A. Beck, 1979; "Rational Emotive Behavior Therapy" by A. Ellis & D. J. Ellis, 2011.

| Thinking Trap | What it looks like? | What triggers it? |
|---|---|---|
| All-or-Nothing Thinking | Not seeing any nuance<br>Binary solutions | |
| Over generalization | "Always" and "never" statements | |
| Mental Filter | Focus on one event and see everything as related to it | |
| Discounting the Positive | Attributing hard work to luck or that your best wasn't good enough | |
| Jumping to Conclusions | Without evidence asserting something is true | |
| Mind Reading | Claiming you knowing someone's internal motivations and thoughts | |
| Magnification | Failing to see problems in context and minimizing your characteristics | |
| Emotional Reasoning | You attribute your emotions to being factual reality instead of a complex web of information | |
| Should statements | Words that indicate obligation, duty, or ingular correct method exist...when no obligation, duty, or singular correct method exists | |
| Labeling | Stating that your actions are your identity | |
| Personalization and blame | You are singularly responsible for an action that has complex inputs that aren't under your control or stating that someone else is singularly responsible. | |

*Figure 2*. Common Thinking Traps Adapted from "The Feeling Good Handbook" by D. D. Burns, 1999.

*Table 1*. Character Strengths. From "Character Strengths And Virtues: A Handbook And Classification" by C. Peterson & M. E. Seligman, 2004.

1. Wisdom and knowledge – cognitive strengths that entail the acquisition and use of knowledge.

- Creativity: Thinking of novel and productive ways to do things; includes artistic achievement but is not limited to it
- Curiosity: Taking an interest in all of ongoing experience; finding all subjects and topics fascinating; exploring and discovering
- Judgment/critical thinking: Thinking things through and examining them from all sides; not jumping to conclusions; being able to change one's mind in light of evidence; weighing all evidence fairly
- Love of learning: Mastering new skills, topics, and bodies of knowledge, whether on one's own or formally. Obviously related to the strength of curiosity but goes beyond it to describe the tendency to add systematically to what one knows
- Perspective: Being able to provide wise counsel to others; having ways of looking at the world that make sense to the self and to other people

2. Courage – emotional strengths that involve the exercise of will to accomplish goals in the face of opposition, external or internal

- Bravery: Not shrinking from threat, challenge, difficulty, or pain; speaking up for what is right even if there is opposition; acting on convictions even if unpopular; includes physical bravery but is not limited to it

- Industry/perseverance: Finishing what one starts; persisting in a course of action in spite of obstacles; "getting it out the door"; taking pleasure in completing tasks

- Authenticity: Speaking the truth but more broadly presenting oneself in a genuine way; being without pretense; taking responsibility for one's feelings and actions
- Zest: Approaching life with excitement and energy; *not* doing things halfway or halfheartedly; living life as an adventure; feeling alive and activated

3. Humanity – interpersonal strengths that involve "tending" and befriending" others

- Kindness: Doing favors and good deeds for others; helping them; taking care of them
- Love/intimacy: Valuing close relations with others, in particular those in which sharing and caring are reciprocated; being close to people
- Social intelligence: Being aware of the motives and feelings of other people and the self; knowing what to do to fit in to different social situations; knowing what makes other people tick

4. *Justice – civic strengths that underlie healthy community life*

- Citizenship/teamwork: Working well as member of a group or team; being loyal to the group; doing one's share

- Fairness: Treating all people the same according to notions of fairness and justice; not letting personal feelings bias decisions about others; giving everyone a fair chance

- Leadership: Encouraging a group of which one is a member to get things done and at the same time good relations within the group; organizing group activities and seeing that they happen

5. *Temperance – strengths that protect against excess*

- Forgiveness/mercy: Forgiving those who have done wrong; giving people a second chance; *not* being vengeful
- Modesty/humility: Letting one's accomplishments speak for themselves; *not* seeking the spotlight; *not* regarding one's self as more special than one is
- Prudence: Being careful about one's choices; not taking undue risks; not saying or doing things that might later be regretted
- Self-control/self-regulation: Regulating what one feels and does; being disciplined; controlling one's appetites and emotions

6. Transcendence – strengths that forge connections to the larger universe and provide meaning

- Awe/appreciation of beauty and excellence: Noticing and appreciating beauty, excellence, and/or skilled performance in all domains of life, from nature to art to mathematics to science to everyday experience
- Gratitude: Being aware of and thankful for the good things that happen; taking time to express thanks
- Hope: Expecting the best in the future and working to achieve it; believing that a good future is something that can be brought about
- Playfulness: Liking to laugh and tease; bringing smiles to other people; seeing the light side; making (not necessarily telling) jokes

- Spirituality: Having coherent beliefs about the higher purpose and meaning of the universe; knowing where one fits within the larger scheme; having beliefs about the meaning of life that shape conduct and provide comfort

# Appendix B

Teaching resilience skills and building psychological safety will increase the well-being and psychological safety of cybersecurity workforce within the federal government.

## Introduction

Resilience skills and building psychological safety have been shown to increase the well-being and productivity of employees (Reivich, Seligman, & McBride, 2011; Edmondson & Lei, 2014). This finding shows that these skills are also trainable. Since the skills to create resilience and psychological safety are trainable this is an opportunity to increase the well-being and productivity of cybersecurity professionals. To measures of increases in well-being and increases The Positive and Negative Affect Schedule (PANAS) and Edmonson 7-item survey are valid scales for measuring well-being and psychological safety respectively (Crawford & Henry, 2004; Edmonson, 1999). Through testing a clear understanding can be reached about the effectiveness of resilience and psychological safety training in increase learning well-being and productivity.

## Methods

Three cohorts would be required to test the hypothesis. All 216 participants would take the PANAS and Edmonson 7-item survey before and after the interventions. All cohorts are randomly assigned. In Cohort 0, 72 participants would be assigned to read a book chapter about professional development. In Cohort 1, 72 participants would attend a traditional lecture about leadership styles in the cybersecurity professional workforce. In Cohort 2, 72 participants will receive training increasing well-being and psychological safety cybersecurity professional workforce. Each cohort's intervention will last 4 days. The three cohorts will then be compared against each other to see which method increased PANAS and Edmonson 7-item survey the most.

**Predicted results**

Cohort 2 will have the most increase in well-being and psychological safety. Cohort 2 is the only group that uses the deliberate practice method. Cohort 0 and 1 should have similar psychological safety and well-being scores.

**Next Steps**

If we can find a correlation between increases in PANAS and Edmonson 7-item scores, we can develop a more extensive randomized study. If those results were promising, we could then make recommendations on how to increase well-being and psychological safety. If the PANAS and Edmonson 7-item scores do not increase together, or one goes down as the other goes up, we can design a study to look at what factors impact well-being vs. psychological safety.