Cyber TrustIQ

Assessing Aptitude. Creating Pathways. Precise Placement.

2015

Identifying Dimensions of Cyber Aptitude: The Design of the Cyber Aptitude and Talent Assessment

Identifying Dimensions of Cyber Aptitude: The Design of the Cyber Aptitude and Talent Assessment

Susan G. Campbell, Polly O'Rourke, Michael F. Bunting
University of Maryland Center for Advanced Study of Language

Cybersecurity is a broad and growing job field, encompassing many different job categories with different cognitive demands. Traditional, knowledge-based assessments may exclude candidates who are cognitively suited to performing cybersecurity work but who have not had the opportunity to learn the subject matter. Using the job categories included in the National Initiative for Cybersecurity Education (NICE) framework for the cybersecurity workforce, we propose a model for predicting cybersecurity aptitude beyond a general-intelligence approach. In addition to including general intelligence, the model is based on a classification of jobs as requiring real-time or deliberate performance, and proactive or reactive actions. We suggest that tasks, work roles, and people can be represented along the same set of axes to match job requirements to person attributes. These constructs can then be used to create assessments of potential for cybersecurity applicants, including one we propose, called the Cyber Aptitude and Talent Assessment (CATA).

The military, the intelligence community, and the private sector all grapple with the problem of recruiting, training, and retaining competent cybersecurity professionals. This challenge steadily increases with advances in technology and sophistication of cyber adversaries. Currently, the best approaches to assessing potential cybersecurity hires involve testing applicants' knowledge of cybersecurity concepts and procedures (Trippe, Moriarty, Russell, Carretta, & Beatty, 2014). Because cybersecurity is an expanding field, however, some applicants who could potentially perform cybersecurity jobs at a high level may not have the required background knowledge when they apply. The challenge, therefore, of cybersecurity aptitude testing is to determine what traits, other than existing knowledge, contribute to success in cybersecurity-related tasks.

One piece of the puzzle for understanding cybersecurity jobs is characterizing what jobs are cybersecurity jobs and how those work roles fit together. The National Initiative for Cyber Education (NICE), which is a project of the National Institutes for Standards and Technology (NIST), is currently in the process of determining what knowledge, skills, and abilities are required for particular cyber jobs, but there is no one ideal worker in the cybersecurity field. The draft NICE framework (NICE, 2014), for instance, covers job titles that include Network Engineers, Developers, Forensic Analysts, and Penetration Testers. These jobs have very little in common besides the fact that they are all classified as cybersecurity jobs and can be part of a cybersecurity team. They do not require the same technical skills, temperaments, or cognitive abilities.

As part of a project to evaluate the cognitive demands of cybersecurity coursework (Golonka et al., 2014), we conducted a literature review on the predictors of cybersecurity job performance and proposed an aptitude test battery for cybersecurity jobs based on a multidimensional model of job performance across a range of cybersecurity job roles and tasks. In this paper, we briefly describe the way our model relates to the measurement of cognitive aptitude for predicting job performance. We then suggest how this model can be turned into an aptitude battery and the future work required to do so.

REVIEW

The best selection instruments available today for cybersecurity training are knowledge tests covering cybersecurity, computer science, and computer networking concepts. These tests are useful for separating applicants who have the appropriate background from those who do not. These sorts of tests include commercial certifications, like the Certified Ethical Hacker exam, and the Air Force's Information/Communications Technology Literacy (ICTL) test, which is currently being validated to become a component of the Armed Services Vocational Aptitude Battery (ASVAB; Trippe et al., 2014).

Because the academic pipeline for cybersecurity is relatively new compared to disciplines like computer science or mathematics, many potential employees will not have the appropriate background knowledge to do well on commercial certifications or tests like the ICTL.

There are several possible approaches to predicting job performance independently of particular pre-existing technical skills. We suggest that a combination of factors predicts performance in cybersecurity work roles: general cognitive abilities, non-cognitive factors (like temperament or personality), specific aptitudes, and specific knowledge.

Cognitive abilities and job performance

General cognitive ability is the best predictor of individual job performance across job categories and situations (Ree & Earles, 1992; Schmidt & Hunter, 1992; Schmidt, 2002). Controversy exists, however, about whether additional cognitive abilities can provide predictive utility beyond general intelligence for particular jobs and situations. One place where specific abilities are likely to be predictive of performance is in situations where initial selection on general cognitive ability already occurs (Lubinski, 2000). In the case of cybersecurity jobs, many employers do select applicants based on general cognitive ability due to the complexity of cybersecurity work.

Non-cognitive attributes and job performance

Though cognitive abilities are the best predictor of performance, assessment of non-cognitive attributes can provide additional predictive power (Schmidt & Hunter, 1998). Such dispositional attributes like tolerance for ambiguity or curiosity can provide information about the fit of applicants for particular types of job.

Specific aptitude tests

The US armed services use the ASVAB as a selection and placement tool. The ASVAB includes measures of general abilities, clustered into mathematical and verbal abilities, plus measures of specific knowledge, like science, mechanical engineering, and automotive maintenance. These measures are combined into different composite scores depending on the requirements for each potential job.

Some military jobs have additional testing requirements beyond the ASVAB. For applicants whose jobs may include a language component, the Defense Language Aptitude Battery (DLAB) is required (Petersen & Al-Haik, 1976; Jackson et al., 2012). The DLAB is a cognitive ability measure, but it taps additional components besides general intelligence that are critical to language learning. For example, DLAB's most predictive subsection taps grammatical sensitivity, which is a specific type of verbal ability (Jackson et al., 2012).

Though these kinds of tests may be related to general cognitive ability, they add prediction related to specific types of processing requirements that particular jobs may have. In comparing a purely ASVAB (general intelligence model) to a model with a separate language aptitude test, Jackson and colleagues (2012) found that the DLAB (or DLAB2) added important prediction of success in language training.

Knowledge tests as aptitude tests

One approach to assessing aptitude and interest in a particular subject with specialized subject matter is to create a knowledge test on that subject matter. As described by Guilford and Lacey (1947), this combined knowledge test approach is used for certain subtests of the ASVAB, including General Science, Electronics Information, and Auto and Shop Knowledge. Guilford and Lacey argued that in the case of informational tests, knowledge could come from any mixture of three factors: interest, aptitude, or opportunity, and thus that tests of job-specific information were a good measure of both interest and aptitude in that area. This approach is also being taken by the Air Force ICTL team, who have developed a knowledge test that predicts performance in cyber training (Trippe et al., 2014).

PROPOSED MODEL

In contrast to a purely general-intelligence-based model, we propose a model of cybersecurity performance with two major components: a critical thinking component, including measures of working memory and reasoning, and a job-specific component that includes measures of particular constructs that match the demands of particular jobs. The job-specific components may include cognitive abilities and non-cognitive attributes. A schematic of the job-specific model, with particular jobs identified, is provided in Figure 1.

Critical thinking corresponds to measures of general cognitive ability, which predict a wide range of job categories. Like

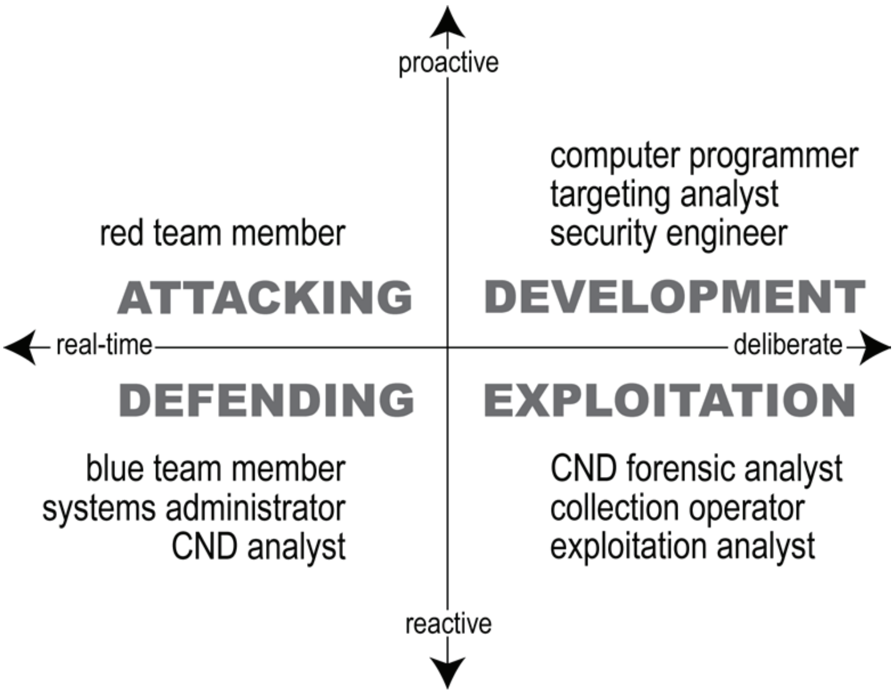

Figure 1. Schematic of the dimensions on which example cyber careers differ. The quadrant names (in bold uppercase font; e.g., ATTACKING) correspond to a major job task that has the characteristics described on its axes (for instance, “defending” requires real-time reaction, while “development” requires proactive deliberation. Example job titles, which appear within quadrants, are taken from the NICE framework.

problem solving in other job categories, solving problems in cybersecurity requires attending to the structure of problems, learning rules, and maintaining goal structures in memory.

We propose to divide particular cybersecurity tasks, and the jobs that predominantly feature those tasks, along two major dimensions: proactive/reactive, and real-time/deliberate.

Proactive activities require the ability to hypothesize the possible outcomes of actions and the ability to come up with creative solutions to problems. These abilities support planning and anticipating consequences. In contrast, reactive activities require vigilance and the ability to detect anomalous activity. They involve being able to recognize problems and react to them, and to see the world as it is rather than as you expect it to be.

Deliberate action is characterized by critical thinking ability and by the ability to defer resolution until sufficient information is available. Real-time action, on the other hand, requires the ability to act quickly and accurately, and to resist distraction. It may require a tolerance for risk when the rewards are important.

These dimensions characterize particular tasks, but a particular job may require tasks that come from different portions of the spectrum. Our model does not require that people fall at a particular point on the grid – a person could be good both at deliberate action when appropriate and real-time action when appropriate. As illustrated in Figure 2, a single task, such as debugging software, may require a certain level of proactive, deliberate action, a particular task may be one of many associated with a particular job, and a particular person may be good along some or all axes. Being good at proactive thinking, for instance, does not necessarily make someone bad at reactive thinking.

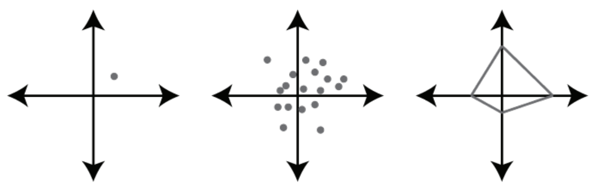

Figure 2. Contrast among use of dimensions for defining a single task as a point, a work role as a combination of tasks, and a person profile as a polygon.

Critical thinking constructs

Based on a review of what has predicted performance in computer science and STEM occupations in the past, we suggest measuring several different aspects of critical thinking: visuospatial working memory, rule induction, complex problem-solving, spatial visualization, and attentional capacity.

Visuospatial working memory has previously been linked to performance in computer science and electrical engineering tasks (Kyllonen, 1996; Hinze, Bunting, & Pellegrino, 2009). Rule induction has been identified as a major component of reasoning ability across domains (Carroll, 1993) and has been used to predict programming ability in novice programmers (Irons, 1982). Complex problem solving is a newer construct that has not been used to predict performance in this domain before, but it is the ability to successfully learn and control tasks that are complex, opaque, and dynamic (Frensch & Funke, 1995). Spatial visualization ability has been shown to predict both performance with computer interfaces (Vicente, Hayes, & Williges, 1986) and long-term achievement in Science, Technology, Engineering, and Math (STEM) fields (Kell, Lubinski, Benbow, & Steiger, 2013). Attentional capacity is a subcomponent of the working memory system which has been shown to be a better predictor of educational achievement than other types of working memory measure (Cowan et al., 2005).

Proactive thinking constructs

The two constructs we have identified to represent proactive thinking are creating mental models and convergent creative thinking. The ability to integrate information into an accurate mental model is a good predictor of STEM learning (Hinze et al., 2013). Convergent creative thinking involves generating atypical associative links between concepts in order to generate a solution to a problem (Cropley, 2006).

Reactive thinking constructs

We represent reactive thinking as responsiveness to the environment, and thus the two reactive thinking constructs we have identified are anomaly detection and vigilance. Anomaly detection involves identifying events that do not conform to an expected pattern, and that type of processing is necessary for many types of cybersecurity task. Vigilance involves effortfully monitoring situations where targets are rare, and monitoring is mentally taxing (Warm, Parasuraman, & Matthews, 2008).

Real-time action constructs

Though cyber actions may be pre-programmed, operators must still make some decisions quickly and accurately. We suggest that psychomotor speed, perceptual speed, and resistance to interfering information will lead to fast and accurate performance in cyber operations. Ackerman (1988) suggested that psychomotor speed reflects differences in the ability to proceduralize tasks. Perceptual speed, especially in recognizing patterns, may also reflect differences in the ability to proceduralize (Ackerman & Cianciolo, 2000). Resistance to interference shows in individual differences in the degree to which earlier information inhibits the ability to deal with new information (Engle, 2002).

Deliberate action constructs

The two non-cognitive constructs we have identified for deliberate action are the ability to delay closure and the ability to weigh risk and reward. The ability to delay closure (the opposite of a high need for closure; Webster & Kruglanski, 1994) allows people to continue difficult information search tasks (Dougherty & Harbison, 2007). The ability to weigh risk and reward is necessary for many tasks involving such balancing.

Test battery structure

A test battery based on these dimensions and constructs should include multiple assessments across constructs that are not highly correlated with each other. Validity testing of the components of this model, therefore, will involve first determining whether a particular candidate test measures the construct it is intended to measure, then determining if the factor

Table 1. Comparison of ability constructs in the model described in this paper with the constructs identified by Trippe et al. (2014) and selected cognitive competencies listed in the NICE Framework.

Constructs in the CATA model	Abilities from Trippe et al. (2014; Table 2)	Cognitive competency areas from NICE
Visuospatial working memory	Verbal reasoning	Mathematical reasoning
Rule induction	Nonverbal reasoning	Modeling and simulation
Complex problem-solving	Mathematical reasoning	Computer skills
Spatial visualization	Problem sensitivity	Reasoning
Attentional capacity	Originality	External awareness
Need for closure	Information ordering	Oral communication
Tolerance for risk	Written communication	Logical systems design
Psychomotor speed	Oral comprehension	
Pattern recognition and scanning	Perceptual speed	
Resistance to interference	Advanced written comprehension	
Modeling program execution	Written expression	
Creativity (convergent thinking)	Near vision	
Anomaly detection		
Vigilance		

structure of these constructs matches the structure described here. Finally, we intend to determine whether the test predicts performance across selected cybersecurity jobs.

Our model is situated at a more general cognitive level than the NICE Framework's Knowledge, Skills, and Abilities (KSA) sections, which, in their current draft form, list only 13 abilities across job titles, compared to 759 items of knowledge and 185 skills.

Though the NICE Framework does not include many cognitive abilities, it does identify several competency areas for skills and knowledge that correspond to constructs we have suggested for our model. In addition to the knowledge constructs Trippe and colleagues (2014) proposed to measure with the ICTL, however, they also identified a number of cognitive abilities that would be required for successful execution of cyber jobs. These constructs include several measures of reasoning and verbal ability. Table 1 shows the list of constructs we identified for this project, alongside the list of abilities identified by subject matter experts in Trippe et al. (2014), and a selected list of cognitive competency areas taken from the NICE framework. The main divergence between our model and the other lists comes in the realm of written and verbal expression, which we had assumed would be assessed either by the ASVAB (in the case of military applicants) or in the interview process (in the case of non-military applicants).

DISCUSSION

We are currently in the process of identifying target populations and situations where a test based on this model could be used to improve selection and training outcomes. Targeted populations include career-switching professionals, university students, and military recruits. Though these populations differ in their type and level of education, for instance, we intend to use longitudinal and cross-sectional designs to determine whether these constructs predict their performance in jobs that require advanced cyber skills.

Applications for selection

Some applicants for cybersecurity jobs will not have the requisite background knowledge, especially if they are transitioning from other fields. A battery based on these constructs could be used to provide supervisors with information about which applicants have the potential to learn to perform a cybersecurity job role.

Applications for training

Students come to cybersecurity training and education programs with a wide variety of backgrounds and ability profiles. This heterogeneity can make teaching and learning difficult; teachers cannot provide all of the relevant background information without frustrating students who have mastered that material already. By assessing aptitude and finding ways to tailor remedial training to a learner's aptitude profile in order to address gaps in skills and knowledge for students who are otherwise likely to succeed, trainers can better place students in appropriate training.

Training pipelines for cybersecurity tend to branch, because there is no one single cybersecurity job role. A multi-branch test could be used to direct people to particular tracks within an educational program. Additionally, the information could be used to structure similar coursework for different audiences.

Summary

Cybersecurity training and selection is still a difficult problem for organizations from small businesses to governments. We are proposing a framework for creating tests, including the CATA, which we have featured here. These sorts of tests combine measures of general cognitive ability and problem-solving ability, which are known to predict performance across job categories, with measures of specific types of cognitive activities and non-cognitive orientations which can specifically affect performance in a range of cybersecurity occupations. The framework allows the connection of tasks to jobs, and the connection of job requirements to applicant aptitude profiles. These dimensions could be altered or added to if necessary to expand the range of tasks and jobs that could be accounted for.

ACKNOWLEDGEMENTS

William Burns, J. Isaiah Harbison, Patrick Cushen, and John Romano all contributed significantly to the concepts behind this research. We would also like to thank our teammates on the Cognitive Support for Cyber Training team here at CASL.

This material is based upon work supported, in whole or in part, with funding from the United States Government. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the University of Maryland, College Park and/or any agency or entity of the United States Government.

REFERENCES

Ackerman, P. L. (1988). Determinants of individual differences during skill acquisition: Cognitive abilities and information processing. *Journal of Experimental Psychology: General, 117*, 288-318. doi:10.1037/0096-3445.117.3.288

Ackerman, P. L., & Cianciolo, A. T. (2000). Cognitive, perceptual speed, and psychomotor determinants of individual differences during skill acquisition. *Journal of Experimental Psychology: Applied, 6*, 259-290. doi:10.1037/1076-898x.6.4.259

Campbell, S.G., O'Rourke, P., Harbison, J.I., & Bunting, M.F. (2014). *Assessing aptitude for cybersecurity training: The Cyber Aptitude and Talent Assessment.* College Park, MD: University of Maryland Center for Advanced Study of Language.

Campbell, S.G., Fiske, T.F., Glazer, S., Foster, J.L., Engle, R.W., & Bunting, M.F. (2013). *Assessing cyber aptitude: An initial model for selecting cyber analysts.* College Park, MD: University of Maryland Center for Advanced Study of Language.

Carroll, J. B. (1993). *Human cognitive abilities: A survey of factor-analytic studies*. New York, NY: Cambridge University Press. doi:10.1017/CBO9780511571312

Cowan, N., Elliott, E.M., Saults, J.S., Morey, C.C., Mattox, S., Hismjatullina, A., & Conway, A.R.A. (2005). On the capacity of attention: Its estimation and its role in working memory and cognitive aptitudes. *Cognitive Psychology, 51*, 42-100. doi:10.1016/j.cogpsych.2004.12.001

Cropley, A. (2006). In praise of convergent thinking. *Creativity Research Journal, 18*, 391-404. doi:10.1207/s15326934crj1803_13

Dougherty, M. R., & Harbison, J. I. (2007). Motivated to retrieve: How often are you willing to go back to the well when the well is dry? *Journal of Experimental Psychology: Learning, Memory, and Cognition*, 33, 1108-1117. doi:10.1037/0278-7393.33.6.1108

Engle, R. W. (2002). Working memory capacity as executive attention. *Current Directions in Psychological Science,* 11, 19-23. doi: 10.1111/1467-8721.00160

Frensch, P. A., & Funke, J. (Eds.). (1995). *Complex Problem Solving: The European Perspective.* Hillsdale, NJ: Lawrence Erlbaum Associates, Inc.

Golonka, E., Clark, M., Karuzis, V., Saner, L., Burns, W., & Haarmann, H.J. (2014). *Recommendations for enhancements to the intermediate cyber core course: A survey-based analysis of cognitive and other demands.* College Park, MD: University of Maryland Center for Advanced Study of Language.

Guilford, J.P., & Lacey, J.I. (1947) (Eds.). *Printed Classification Tests* (Army Air Forces Aviation Psychology Program Research Reports series, Report No. 5). Washington, DC: Army Air Forces.

Hinze, S. R., Rapp, D. N., Williamson, V. M., Shultz, M. J., Deslongchamps, G., & Williamson, K. C. (2013). Beyond ball-and-stick: Students' processing of novel STEM visualizations. *Learning and instruction, 26*, 12-21. doi: 10.1016/j.learninstruc.2012.12.002

Hinze, S. R., Bunting, M. F., & Pellegrino, J. W. (2009). Strategy selection for cognitive skill acquisition depends on task demands and working memory capacity. *Learning and Individual Differences, 19,* 590-595. doi:10.1016/j.lindif.2009.07.008

Irons, D. M. (1982). Cognitive correlates of programming tasks in novice programmers. In *Proceedings of the 1982 Conference on Human Factors in Computing Systems* (pp. 219-222). New York, NY: ACM. doi:10.1145/800049.801783

Jackson, S.R., Silbert, N.H., Campbell, S.G., Hughes, M.M., Smith, B.K., Tare, M., … Bunting, M.F. (2012). *The operational impact of DLAB2: Summary of recommendations and success-rate simulation.* College Park, MD: University of Maryland Center for Advanced Study of Language.

Kell, H. J., Lubinski, D., Benbow, C. P., & Steiger, J. H. (2013). Creativity and technical innovation: Spatial ability's unique role. *Research Report, 24*, 1831-1836. doi:10.1177/0956797613478615

Kyllonen, P. C. (1996). Is working memory capacity Spearman's g? In I. Dennis & P. Tapsfield, *Human abilities: Their nature and measurement.* Mahwah, NJ: Lawrence Erlbaum Associates, Publishers.

Lubinski, D. (2000). Scientific and social significance of assessing individual differences: "Sinking shafts at a few critical points." *Annual Review of Psychology 51,* 405-444. doi:10.1146/annurev.psych.51.1.405

National Initiative for Cybersecurity Education (2014). *DRAFT National Cybersecurity Workforce Framework Version 2.0.*

Petersen, C.R., & Al-Haik, A.R. (1976). The development of the Defense Language Aptitude Battery (DLAB). *Educational and Psychological Measurement 36*(2), 369-380. doi:10.1177/001316447603600216

Ree, M.J., & Earles, J.A. (1992). Intelligence is the best predictor of job performance. *Current Directions in Psychological Science 1*(3), 86-89. doi:10.1111/1467-8721.ep10768746

Schmidt, F.L. (2002). The role of general cognitive ability and job performance: Why there cannot be a debate. *Human Performance 15*(1-2), 187-210. doi:10.1080/08959285.2002.9668091

Schmidt, F.L., & Hunter, J.E. (1992). Development of a causal model of processes determining job performance. *Current Directions in Psychological Science 1*(3), 89-92. doi:10.1111/1467-8721.ep10768758

Schmidt, F.L., & Hunter, J.E. (1998). The validity and utility of selection methods in personnel psychology: Practical and theoretical implications of 85 years of research findings. *Psychological Bulletin, 124*(2), 262-274. doi:10.1037/0033-2909.124

Trippe, D.M., Moriarty, K.O., Russell, T.L., Carretta, T.R., & Beatty, A.S. (2014). Development of a cyber/information technology knowledge test for military enlisted technical training qualification. *Military Psychology 26*(3), 182-198. doi:10.1037/mil0000042

Vicente, K.J., Hayes, B.C., & Williges, R.C. (1987). Assaying and isolating individual differences in searching a hierarchical file system. *Human Factors 29*(3), 349-359. doi:10.1177/001872088702900308

Warm, J. S., Parasuraman, R. & Matthews, G. (2008). Vigilance requires hard mental work and is stressful. *Human Factors, 50*, 433-441. doi:10.1518/001872008X312152

Webster, D. M. & Kruglanski, A. W. (1994). Individual differences in need for cognitive closure. *Journal of Personality and Social Psychology, 67*, 1049-1062. doi:10.1037/0022-3514.67.6.1049

Assessing Aptitude. Creating Pathways. Precise Placement.

Identifying Dimensions of Cyber Aptitude: The Design of the Cyber Aptitude and Talent Assessment

CONTACT

A: Research Triangle Park North Carolina
E: info@cyber-alliance.com
T: (984) 293-7628