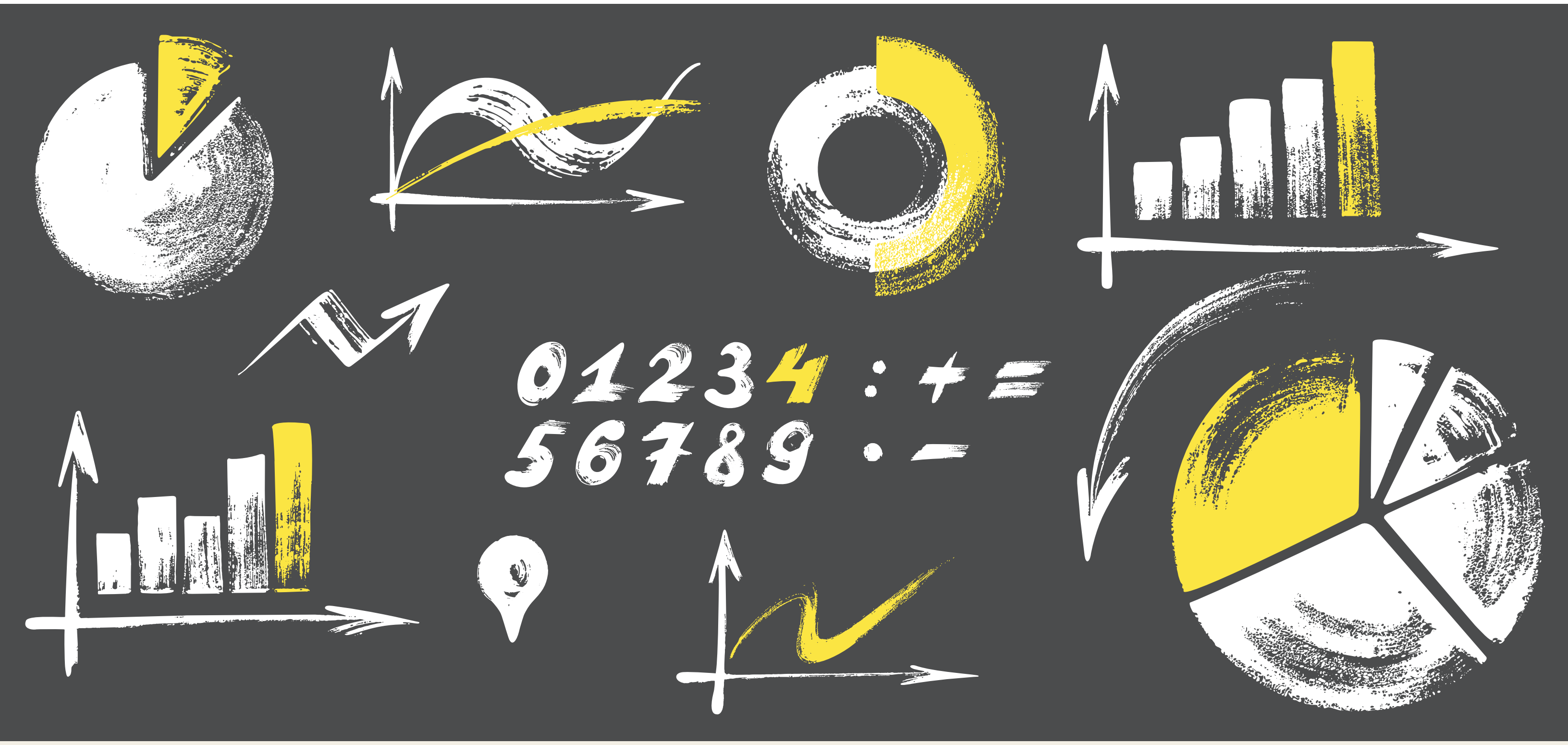
# JOURNAL OF WOMEN AND MINORITIES IN TECHNOLOGY

ISSN: 2640-8015

Volume 1, Issue 2



As we move into 2020 we continue to see great opportunities for women and minorities to be actively recruited by organizations across the country and the world. This first issue of Women and Minorities in Technology this year covers some interesting topics in several areas of technology. We will continue to provide articles written by academics and professionals in the fields of aviation, nuclear, cybersecurity, and information technology. Our continued goal is to share timely information that is of interest to women and minorities interested in technical careers.

*Founding Co-Editors: Jane LeClair, EdD and Tanis M. Stewart, PhD*

THOMAS EDISON STATE UNIVERSITY
School of Applied Science and Technology

## Table of Contents

## EDITORIAL BOARD

### Founding Co-Editors

## PEER REVIEWERS

The Women and Minorities in Technology Journal gratefully acknowledges the reviewers who have provided valuable service to the work development of the journal:

### Peer Reviewers

# Modular AI Vehicle Security and Support (MAVSS): Holistic Cybersecurity Approach

Dr. Charles Parker II

Nikolas Upton

Vehicles are and have been for decades an integral facet of the nation’s culture. Consumers spend hours with their vehicles, these are prominently placed in movies, songs, and other cultural aspects. There are vehicles in cartoons and advertisements from the 1960’s and 1970’s, indicating there will be flying cars in the future. In the Saturday Evening Post from the 1950’s, the driverless vehicle was advertised (Weber, 2014).

After years of thought, creativity, design, and engineering, the vehicle’s functionality has advanced. The prior rendition of the vehicle was a mechanical beast, requiring several mechanical engineers and one electrical engineer. The innovations and advances inversed this ratio. The increase in electrical engineers is required as the vehicle moved from primarily being mechanically focused to a greater level of interaction with the user and implementation of electronics.

In particular, the users demanded through their financial voting to purchase advanced vehicles integrated with their personal electronics and devices and offered interactions with the world outside of the vehicle. These include music services, maps, phone calls, texting, and the various other functions. At present, the industry and vehicle environment is at the cusp of autonomous drive (AD) vehicles actively being driven on the road, where the driver doesn’t need to engage with the vehicle’ operation or other drivers on the road. The vehicle’s sensors and operating system (OS) will manage the systems and driving, as the vehicle moves toward the user’s destination thereby automatically interacting with other vehicles (V2V) and the vehicle to infrastructure (V2I). To engineer this functionality to not only operate but also with safety and security integrated through the software development lifecycle (SDLC) requires teams of electrical engineers, software engineers, cybersecurity engineers, and other technical specialties, along with a few mechanical engineers.

The advancing technology has been experienced by the general public in the past with vehicle’s anti-lock and key entry system. The vehicle’s key lock and entry system started with the physical, metal key. This tool was upgraded to a push button system (Gill, & Sachin, 2016). Now, with near field communication (NFC), a user can simply walk up to the vehicle and is able to open the door. There is now a biometric fingerprint scanner, which is already being used as a security feature in other industries for over a decade. This technology has already proven itself to be viable and proficient.

The minimalist statement on a Connected and Autonomous Vehicle (CAV), that it is able to drive itself, while simplistic, still requires a certain level of definitions. The vehicle manufacturers will still need to improve the CAV technology with strengthened sophistication, complexity of modules and sensors in the operation within the confines of the vehicle (Lima, Rocha, Volp, et al., 2016). The CAV will also require constant communications with other vehicles using V2V, the infrastructure when time- and technology-appropriate (V2I), and other germane equipment relevant to the vehicles operations within and with other vehicles (V2X). The intra-vehicle communication involves the sensors located throughout the vehicle, internal and external. The sensors within the vehicle act as a gateway for the real-world (Shin, Son, Park, et al., 2016). The sensors that are strategically located throughout the vehicle provide the input which is processed through the vehicle's on-board computer and are vital to the CAV.

While there is a benefit for the user experience (UX), this presents distinct issues associated with this form of vehicle operation. As the operation would be autonomous, an attacker hijacking the vehicle has the distinct potential to be a critical event not only for the vehicle, but also the entirety of the users within and proximate to the vehicle. The CAV vehicle's operations have to be secure and safe. There is no alternative. To provide a safe platform for the CAV vehicle operations, there needs to be a secure OS, which is focused not only on the UX, but more importantly to the users, on cybersecurity to ensure the vehicle and its modules may not be effectively attacked or compromised. The proposed OS will function to this end, to protect the vehicle, and user(s) within the vehicle.

## Attack Points

These sensors need to be able to completely communicate at all times with other sensors and systems logging functions. Any lag or disruption would represent a problematic situation. The various sensors located throughout the vehicle provide data points, which the vehicle analyzes to create a 3D map of the surrounding area. If the CAV is not able to function correctly then it could possibly would not have the required data and information to safely operate and drive on the roadway autonomously or with other vehicles present. The insecure CAV provides for the opportunity for significant physical damage to be done to the vehicle (Bezemskij, Loukas, Anthony, & Gam, 2016).

The CAV would be operating virtually blind, which is considered to be an attack point. The data pool, which the CAV uses to interact with the environment, would be empty, partially empty, or filled with misleading data. This attack point can be present with each sensor within the entire vehicle. The attacker could possibly choose the sensor that requires the least effort for compromise, providing the greatest Return On Effort (ROE) expended. The attack may then pivot from one component to other vehicle systems. Unfortunately, with each successful attack, there would be increasingly detrimental effects to the vehicle, its operations, and eventually the passenger's health and safety. Damage and compromise to these sensors may also provide for attackers to conduct vehicle theft (Omanakuttan, Sreedhan, Manoj, et al., 2017).

## Detection and Mitigation

The capability and persistence of attackers are so much of a threat to the vehicle industry that sensors and other vehicle systems related activities should be fully secured from unauthorized access and manipulation. The historic attacks have been centered on three aspects of sensor operations-software, network, and spoofing (Shoukry, Nuzzo, Pugelli, Sangiovanni-Vincentelli, Seshia, & Tabuada, 2015). With software, there may be malicious applications operating within the sensor, may forward incorrect frames/messages, or not send these. The network as the attack point provides for the backbone communication may be targeted, or the packets may be adjusted for the attacker's malicious intent. One example of this is spoofing, which involves the attack providing false data to the sensor. The sensors are vulnerable to manipulating GPS for the attack (Shin, Son, Park, et al., 2016). The typical yet devastating example of this involves GPS spoofing. The attacker would send a signal indicating the vehicle is in Panama, when actually they are in Oxford, OH. These would be manifested as contactless attacks (Yan, Xu, & Liu, 2016). The detecting the unauthorized access and malicious manipulation is the primary initial step, which has been problematic (Shoukry, Nuzzo, et al., 2015).

## Prior Research

The prior detection methods have focused on different aspects of the system. Shoukry, Nuzzo, Puggelli, et al. (2015) researched detection in a linear dynamical system. The researcher's theory termed this secure state estimation. This detection involved each sensor as this would be attacked, while mitigation is more concerned with the state of the module or system being attacked and the subsequent malicious messages/frames.

Spoofing input data is troublesome to the vehicle for several reasons (Son, Shin, Kim, et al., 2015). The researchers investigated attacking drones utilizing the Micro-Electro-Mechanical Systems (MEMS) gyroscope. The research indicated the spoofing did negatively affect the drone applications. This was evidenced by 18 of the 20 drones losing control and crashing. The research answered the hypothesis of whether this was possible. The countermeasures were noted as physical isolation, differential comparator resonance timing. One limiting aspect to the research was the detection and defenses were based on the researchers limited parameters.

Davidson, Wu, Jellinek, et al. (2016) also researched unmanned aerial vehicles (UAV) spoofing attacks. The research indicated the noted attacks were effective. The primary defensive measure for the researcher's theory was the RANSAC algorithm.

Yan, Xu, and Liu (2016) researched contactless attacks against autonomous vehicles. The researchers noted the difference between a traditional form network and networks in the autonomous vehicles. The autonomous vehicles depend heavily on the sensors to assist these in analyzing the environment for driving decisions. For the study, the researcher's target was a Tesla Model S. The researchers in the use case were successful with spoofing and jamming attacks.

## Holistic Approach

The attempt to create the cybersecurity protocol and application has been in the design mode for well over a decade. Nearly all of these efforts have been fruitless. There are a number of companies in the market conducting proof of concept (PoC) testing to understand how to mold their system into a vehicle's network, communication network, and protocols. There has not been a cybersecurity system designed with the focus on embedded systems as part of the environment. The prior attempts have designed a system and attempted to force this into the embedded system.

The present companies have viewed this function as static or the simple input/output issue to be managed by one transaction. As for the former, the companies view the vehicle as a quasi-castle or stronghold. The application is analogous to the medieval era castle walls, seemingly impregnable. During this period, there were periodic attacks against the static castle walls, which were exceptionally effective. Samples of these include, however are not limited to, fire, battering rams, ladders, catapults, and others (History on the Net, n.d.).

Other companies view this as a more simplistic transaction. In the case with a malicious or erroneous message/frame, in theory the system would detect the issue, and simply remove this from the communication channel. When the input is deemed as not appropriate, this is removed from the communication or data flow. While one-dimensional, this does not take into account the operational required communications and essential intra-vehicle communications.

The problematic portion with these has been and continues to be the overly narrow simplistic application of the potential uses of the creativity and technology. Cybersecurity is not a quick transaction or an application to be bolted on at the end of the project. The CAV and its safety implications require much more thought, effort, and application of resources. The cybersecurity application needs to be presented with much more than this. With the level of applicable, viable technology available, this should be implemented.

These present applications detect the attack or message/frame sent in error and remove this from the equation. The method may have worked in the earlier days of vehicle attacks or with an attacker lacking imagination, motivation, or an updated knowledge of exploiting vulnerabilities. There are proofs of why this is Kevorkian-esq design cannot possibly work. It comes down to inverting filter patterns and inherent properties of static filters. There are two problems with static (single step) filters. 1. All static filters (when configured correctly) are "If match then allow else try next case" where at the end of the list of cases the packet/frame/command is dropped. This has many flaws such as truncation, misuse of matches to still complete the commands (trojan horse type) or overwhelming the matches to only filter some (like a sports stadium with their metal detectors. easy to slip by in all the confusion without getting checked) 2. All cases in the set of matches cannot possibly be truly inclusive of desirable matches while being truly exclusive of non-desirable non-matches.

This approach either ceases at this point or logs the event. In the case of spoofing, there has been engineered into the system minimal effort to ensure the sensor inputs are valid. The single step application of cybersecurity will not operate significantly well in the future environment with CAV in vast numbers on the roadways through the nation.

With the level of technology available for this application, additional processes and learning by the modules and nodes are warranted. The machine learning (ML) / artificial intelligence (AI) application to vehicle cybersecurity is applicable, yet has not been adequately explored. ML/AI provides for decision-making, deeper understanding of the data and implications, and issue detection and reporting in a timely manner. While AI is not at the appropriate technological level to be placed solely in the vehicle system for management, this is improving constantly and has a place in the vehicle system.

## MAVSS (Modular AI Vehicle Security & Support)

MAVSS is a new application of present-day technology. It allows for future ML/AI technology to be incorporated and applied in the future. However, as this type of AI technology advances it needs to be tested and vetted for appropriate placement. The testing will provide a deeper understanding and appreciation of the transaction in the vehicle communication channels. The new application of technology will also require additional process overhead. This is engineered not to be a significant detriment to the vehicle's or passenger's safety and operations. As this or a like system is incorporated into the CAV, this processing time, would become the baseline.

This new system is modular in form. The vehicle manufacturer may apply all or part of the MAVSS vehicle cybersecurity system. Based on the use case and target vehicle, there may not be the need for the entire system due to the OEM's needs or parameters. The system likewise is agnostic, as this may be applied to any vehicle platform.

The methodology focuses on quick decision-making. This is required for the vehicle's basic operations. Any new system cannot create a significant time lag. This is also required if the vehicle were to be under attack, especially in the case with contactless modes of attack.

The new cybersecurity system is based on a biological model. With any organism there is the potential for an infection. This may be from a break in the skin or exoskeleton, or an ingesting an item. The organism does not take the stance of the skin, exoskeleton, or body being impregnable or perfectly secure from an infection. The exterior is not and would never be perfect. The body takes into account there will be breaches in the system. The physiology manages the task. The body is consistently looking for attempts to break the exterior to enter the organism. The function is analogous to a vehicle cyber-attack. The infection is analogous to a compromise. The infection point is the attack vector used to compromise the system within the vehicle. Once the breach in the vehicle's OS is detected, the issue would be communicated to the other resources to complete the removal of the issue. MAVSS is no different in its design and application for this holistic defense.

AI/ML is applied to the embedded systems and sensors in CAV. MAVSS was not architected to be a simple “If this then that” algorithm. This basic application is not a workable solution for the vehicle systems. The learning is for a baseline of level of communication between the modules and ECUs and is the starting point (Bezemskjj, Loukas, Anthony, & Gan, 2016). The methodology is a common application with ML/AI. The systems learn the vehicle’s baseline activity, messages, and expected activity for a vehicle, fleet, or platform through the vehicle’s operations and files from the OEM detailing the expected message sequential patterns. The tasks are completed at the manufacturer, and through user driving through applying ML with linear regression. The data cleaning is done to remove any potential out of context messages. These should not be present as they may be unexpected, in error, or simply malicious in nature.

These messages or frames would be manufacturer provided. The OEM engineered the product and  know the protocol and general timing of events and messages. As an example, when the user is making a left turn, there are a number of steps prior to the vehicle turning. These steps would need to be present in order for the vehicle to make the left-hand turn. Each respective OEM would provide their CAN database (Evenchick, 2013). The database has the OEM messages and signals. These are also known as the OEMs DBC or CAN DBC files (CSS Electronics, n.d.). These generally are specific per each OEM. These provide the expected messages and signals, and timing. This is not perfect, however, is an exceptional resource. The data provides the required significant amount of data. There would be empty spaces in the data and timing, which would be filled in by the actual data from the vehicle operations.

For each OEM, the user or an agent for the OEM would need to operate a vehicle for three to four days. The time is required to capture a sufficient level of data and messages to provide an appropriate level of data for analysis and incorporation into the cybersecurity framework. The time would provide for the messages that would be encountered by the vehicle in most all of the use cases. The number of vehicles required would be dependent on the OEM. If the entirety of the fleet uses the same set of CAN messages, the required number of vehicles would be limited to approximately under seven, based on the learning model along with the number of messages. If the fleet were to use different CAN messages, there would need to be the same number required of vehicles per each set.

The process would be on-going with the user, as they would operate the vehicle. The task would function to assist MAVSS with learning over time from the user’s day to day operations. The data acquisition would apply also regression analysis. As each day passes, the increase in data and analysis provides a greater level of understanding of the standard communications and appropriate timing of these. With each day, the cybersecurity system would improve due to the amount of increased data and the subsequent analysis.

As noted, the system is designed to be holistic in structure and defensive in posture. MAVSS is designed to holistic as this is not analyzing the vehicle as an impregnable castle, or static in nature, but more of a dynamic tool for the entirety of the vehicle's operations. Historically, the static model has not worked exceptionally well. The static target provides attack points, which may be researched at length, due to the structure not changing or adjusting itself, and not communicating with each other. There were significant difficulties with the present offerings for cybersecurity applied to vehicle systems. The cycle is analogous to the enterprise attack cycle, with the Admin creating a solution. The defense tends to work well for a limited amount of time. The attackers find another vulnerability to exploit. The Admin creates a new solution for the vulnerability, and the cycle continues.

For the vehicle use case, the dynamic system is required. The dynamic learning from its environment, sensor data, and intuitive nature as to these inputs would provide a much more difficult target to successfully attack. The MAVSS form is based on nature-oriented platform. There is a Central Brain with extensions monitoring and making decisions. This is analogous to an octopus. There is a central brain managing the overall animal. The extension brains manage the local issues. If an issue is presented the extension brain is not able to manage, this is reported to the central brain.

## General Structure

MAVSS is engineered with a Central Processor (CP) and External Nodes (XT Nodes). The Central Processor (CP) functions as the primary/central brain. The CP manages the overall processes and decisions which need to be adjudicated above the local process (XT Nodes). The XT Nodes are external to the central processor. The XT Nodes manage daily operations, questions, and issues, and is connected to the Central Processor. The XT Node function is to complete the initial processing and decision-making. If there were to be a significant issue, which is not able to be managed locally, the issue would be directed by the central processor (CP) for metanalysis. The organization for MAVSS may be physical or virtual, dependent on the manufacturer's parameters. This may include physical XT Nodes, or these formed in a virtual machine (VM) with a hypervisor to manage these.

### Operations

The Central Processor receives the data from the XT Nodes at regular intervals and when there is an issue with the messages/frames. The XT Nodes forward the general log data at regularly scheduled intervals, and when there is an issue with the messages/frames. The process functions to analyze the data from the XT Nodes, any correlations between nodes and the subject activity. The correlation analysis reviews for anomalies, equipment errors, and any message/frame directing an action outside of a margin from the regression analysis and model. Any of these found to be an issue are triaged. The system decides the best course of action with the issue. The issue management would take into consideration safety first. In summary, the operations would be managed at the central processor level first. If the process were not to be able to be resolved at the vehicle level, the issue and logs would be sent to the OEM over the air (OTA) securely.

The logging and analysis is a pertinent function of the MAVSS system. The XT Node logs detected attacks, anomalies, and unusual activities. The general log is forwarded to the central processor at a predetermined rate. The central processor uploads to the cloud at a predetermined rate. The cloud application analyzes the data per OEM's needs, and product line. The process is completed on various levels to review for issues. This data is analyzed alone, from day to day, week to week, against others in the state, region, and country. The system would function to not only analyze the data from the vehicle, but also other vehicle's data to analyze for any potential trends, i.e. attacks against fleets, or groups of vehicles.

The error log itself is received by the central processor. The issue and data had been already triaged and compiled by the XT Node. The red-flagged issues are handled differently than the standard issue.

### XT Node Interaction with Sensors

The XT node, as a natural course of action, completes routine plausibility tests based on the sensor data and reality. The test is to ensure the data from point to point is viable and physically attainable. The analysis is a complete process, and not a boilerplate action. For each sensor, the generic, general test would be the same overall process. The testing however would be specialized for each sensor's data and functionality. The testing itself would compare the prior and current data points for plausibility. The GPS function, as an example, would verify the vehicle's current geographic point and compare this to recent prior points for a reality check, taking into account the trend analysis, including drift, and regression analysis.

As an example, the user is driving to East Lansing, MI. There is the average traffic flow on I-69. The GPS is operating appropriately. The vehicle begins to receive two GPS satellite signals much stronger than the others. Within a minute these signals are the strongest. The GPS signals indicate four minutes later the vehicle is in Colorado. The XT node detects this clear issue and registers this as an anomaly for further review and analysis the anomalous GPS signals continue. The XT node also continues to monitor the signals. The XT node cannot reconcile the present GPS coordinates with the most recent coordinates occurring prior to the GPS signals creating the issue. The vehicle has failed the plausibility and drift tests, along with the regression analysis, taking into consideration any drift, and comparison tests. With the autonomous vehicle, this is a critical issue, which needs to be managed immediately. This functions as the plausibility test for the GPS module.

The module would operate per the OEM directive. These options include the vehicle depending on the other sensors, e.g. LiDAR and radar, immediately and continuing to travel on the safe route. The V2V would also act to compensate for the loss of the GPS signal. In the case when the attack/issue is no longer present, the systems receiving the subject data would return online and processing the data and implementing the noted data.

As for the vehicle's administrative processes, MAVSS CP would forward the relevant portion of the log (e.g. time stamps, geographic data for the seven prior recordings and erroneous recordings, etc.) to the OEM for review and may direct other vehicle actions. This would also be analyzed as part of the data pool.

If at any point, the operations would not be safe for the vehicle and users, the ML/AI UX interface would contact the users to instruct them to take control of the vehicle operations. At a certain point when the vehicle would be out of range of the faux GPS signals, the GPS data and input could be placed back into the data used to guide the vehicle. The ML/AI module addition adds a needed layer of analysis, and decision-making to increase the UX, safety, and value for the user. This addition benefits the individual vehicle, driver, passengers, and other vehicles. The MAVSS adds this along with the traditional security.

## O/S Hardening

There is the distinct need to control the access to the system, processes, and other parties within the vehicle's OS (Sigg, 2011). The standard applies the principle of least privilege. If the O/S is vulnerable or susceptible to attack and compromise, the other sensors, modules, ECUs, and vehicles may not trust the specific equipment or any of the messages or data generated by it. There may be an unauthorized person or another application controlling the messages, and subsequently the vehicle and its operations. Any trust with the compromised system would be a fallacy at best.

The intent with MAVSS is to prevent the issue, deter the attack, create a vehicle cybersecurity environment in which the compromise would be excessively complex and difficult in comparison to other potential targets, and in general create a secure center of operations for the vehicle. The attributes have been designed to accomplish this via incorporating ML/AI into this to secure the O/S and overall system. The defense is required. This in effect would act as a communication gateway, secured from unauthorized entry and communication.

Although the focus is a complicated issue, the methods to accomplish this furtherance for security are known, have been implemented, and are robust. The standards use generally accepted methods. Concerning the checks and counter-checks the redundancy should be implemented at certain critical points at the appropriate level. The action also functions to reduce any potential waste of resources. The system is designed to incorporate the required functions as needed. The system reduces the redundancy, processing overhead (hardware and software requirements, and heat generation), and financial costs.

The methods are partially borrowed from the enterprise cybersecurity defensive systems. The methods would include a firewall-type function to protect the system from any malicious inbound and outbound traffic. The tool may be used presently as part of the defense in depth. In the longer-term, the functions may be supplemented by other tools, which would work better in the vehicle environment. The addition would act as a wall between the internet and internal structure (IBM, n.d.). The defense in depth is necessary to protect the system (Bach & Alshammari, 2013). The intent is to prevent any unauthorized access to the system. This would use a stateful firewall, as this inspects the packets and tracks the TCP connection (Bach & Alshammari, 2013). The configuration would be done with security in mind. Specifically, the security would receive messages from the limited number of known and approved IP addresses. The list would not be published externally to the OEM, Tier 1, or Tier 2 manufacturer or be available by unauthorized parties. Within the application, the IPs are whitelisted. Only the trusted sources involved and are allowed to interact with the vehicle. Any updates to this are secured and encrypted. These are updated at the dealership or OTA (e.g. FOTA or SOTA, dependent on the use case). Only the digitally signed packages are accepted.

Within the vehicle cybersecurity application, the IP address could be spoofed. While the attack is  a viable method, the defense-in-depth counter-measures would be the effective remediation. The defense in depth for the vehicle and system allows for a redundancy in the case of a spoofed IP address, for instance. The attack may be able to move through one safeguard, however, would be detected by one of the other redundant systems. The other systems are engineered to analyze their respective area of operations for unusual activity.

In the scenario where the attacker was able to bypass the entirety of the security controls, and their lateral movement within the vehicle not be noticed, one action they may work towards is exfiltrating the software, firmware, keys, etc. The system would also be reviewing outgoing traffic to ensure the messages were routed to approved IP addresses only. The data volume would also be checked for plausibility prior to being sent. For example, if the expected daily log traffic was expected to be 750G, and on a Thursday a 3T file was attempted to be sent, the system would pause the traffic to review the significant differential. The data would be forwarded to the central processor, and later forwarded to the cloud for analysis.

The files also are a target for the attackers. The attackers may want to temporarily park data in a file in the vehicle for exfiltration at a later date, as they accumulate the targeted data or information. The MAVSS knows what files are to be on the system and their estimated size. The system would compare files within the whitelist to verify the estimated size, and only the files are present that are supposed to be. This would not be a constant function, however, would be completed periodically. As these issues are detected, the data would be forwarded to the central processor by the XT node.

MAVSS would also have a distinct knowledge of the ECUs and their respective configuration. The system would periodically check the whitelisted configuration for each ECU (e.g. authorized open ports) against the actual ECU configuration. The configuration would likewise not be a constantly operating function, but reviewed periodically (i.e. the 15th of the month or the next day the vehicle is on). As these issues are detected, the data would be forwarded to the central processor by the XT node. The applications within the vehicle ecosystem would be known and delineated. These would also be checked at the same time to ensure any unauthorized applications would not be present.

At times, the firmware and software may need to be updated. The FOTA or SOTA updates require authentication to verify these are from the trusted sources. There are several vendors who have created and vetted a solution for the issue, including Red Bend (Ahmed, 2016). The MAVSS would integrate an authentication process into the system.

There would also be user data stored in the system. Dependent on the use case for the particular vehicle line, this may be sensitive data or data logged from the vehicle operations. The data stored within the vehicle system creates an issue, when coupled with the GDPR and other US state's focus on passing laws which address the consumer's need for privacy. The data would be required to be encrypted (Six, 2012, p. 73). This may take several forms, however, would need to be of the current industry standard. The vehicle system using an outdated, vulnerability ridden encryption standard is of no assistance.

## Event Trigger

At the XT Nodes, at times there are safety triggers for the vehicle. The safety triggers would be automatically addressed. From a biological aspect, the regular process is relatively clear. Input from the finger is sent to the spinal column, forwarded to the brain for processing, and the message redirected back to the finger via the same route for an action or inaction. There are certain inputs that are defined as being critical to the organism's well-being. In these emergency situations, an immediate reaction is required. If this is not done, the external issue may destroy tissue or kill the organism.

In these safety critical cases, (e.g. touching fire), the organism retracts the finger immediately prior to the message being sent to the brain for processing and a decision being returned. Within the vehicle, the issue may physically manifest itself as the vehicle being in an accident and the air bags being deployed. As the accident occurs, the vehicle occupants would not want the message delayed with the message being processed at the XT Node, triaged and recognized and not being able to be processed, forwarded to the central processor, processed and decisioned, and forwarded back to the XT Node for processing. In the specific case, the message would not be delayed. The message would continue without being processed so the airbags would be deployed, and other safety features implemented. The event would be fully logged as part of the natural process.

## Closing

As technology improves and advances, so has the CAV. These vehicles will be actively on the roadways in greater numbers in the near future. To ensure these vehicles are safe and secure, cybersecurity has to be applied. The researched option, MAVSS, is proposed to manage this function. The system provides a defense in depth, with an over-abundance of caution at critical points. The defense in depth will be required as the industry continues to move towards the full integration of AD vehicles. The tool or a like functioning tool will be a direct or indirect requirement for the autonomous drive vehicles.

While the project is substantial, the research and coding continue. The task involves not only the functionality for the program, but also for the vehicle and occupant's safety. Without the trust, the CAV will not be a usable product. MAVSS protects the vehicle and occupants in redundant layers of cybersecurity, addressing the different systems. Future research and coding will address the V2V, and V2I, as these are likewise pertinent for securing the vehicle.

## References

Ahmed, M. (2016, August 15). OTA software updates now serving ECUs for engine, brakes, and steering. Retrieved from http://www.embedded-computing.com/embedded-computing.com/embedded-computing-design/ota-software-updates-now-serving-ecus-for-engine-brakes-and-steering

Bach, C., & Alshammari, M. (2013). Defense mechanisms for computer-based information systems. *International Journal of Network Security & Its Applications, 5*(5), 107-113. doi:10.5121/ijnsa.2013.5509. Retrieved from https://www.researchgate.net/publication/259341660_Defense_Mechanisms_for_Computer-Based_Information_Systems

Bezemskij, A., Loukas, G., Anthony, R.J., & Gan, D. (2016, December). Behavior-based anomaly detection of cyber-physical attacks on a robotic vehicle. In *Ubiquitous Computing and Communications and 2016 International Symposium on Cybersecurity and Security (IUCC-CSS), International Conference* on (pp. 61-68). Retrieved from http://gala.gre.ac.uk/15819/7/15819%20Bezemskij_Behavior-based_Anomaly_Detection_2016.pdf

Bhat, C. (2018, February). Cybersecurity challenges and pathways in the context of connected vehicle systems. Retrieved from https://ctr.utexas.edu/wp-content/uploads/134.pdf

CSS Electronics. (n.d.). CAN DBC file-convert data in real-time. Retrieved from https://www.csselectronics.com/screen/page/dbc-database-can-bus-conversion-wireshark-j1939-example/language/en

Davidson, D., Wu, H., Jellinek, R., Singh, V., & Ristenpart, T. (2016, August). Controlling UAVs with sensor input spoofing attacks. Retrieved from https://www.usenix.org/system/files/conference/woot16/woot16-paper-davidson.pdf

Evenchick, E. (2013, October 23). CAN hacking: The in-vehicle network. Retrieved from https://hackaday.com/2014/10/22/can-hacking-the-in-vehicle-network/

Gill, K.R., & Sachin, J. (2016). Vehicle ignition using fingerprint sensor. *International Journal for Innovative Research in Science & Technology, 2*(12), 357-363. Retrieved from http://www.ijirst.org/articles/IJIRSTV2I12043.pdf

Grey Campus. (n.d.). Phases of hacking. Retrieved from https://www.greycampus.com/opencampus/ethical-hacking/phases-of-hacking

History on the Net. (n.d.). Medieval castle defense and assault. Retrieved from https://www.historyonthenet.com/medieval-life-attacking-and-defending-a-castle

IBM. (n.d.). Network security options Retrieved from https://www.ibm.com/support/knowledgecenter/ssw_ibm_i_72/rzaj4/rzaj45zgiptraffic.htm

Kumar, KN, & KR, S. (2018). U.S. Patent Application No. 2018/0278628A1. Washington, DC: U.S. Patent and Trademark Office.

Lima, A., Rocha, F., Volp, M., & Esteves-Verissimo, P. (2016, October). Toward safe and secure autonomous and cooperative vehicle ecosystems. In *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*, pp. 59-70. doi:https://dx.doi.org/10.1145/2994487.2994489. Retrieved from http://orbilu.unilu/bitstream/10993/28773/1/cps03-limaA.pdf

New Wave Design and Verification. (n.d.). Cyber security. Retrieved from https://newwavedv.com/markets/defense/cyber-security/

Omanakuttan, A., Sreedhar, D., Manoj, A., Achankunju, A., & Cherian, C.M. (2017). GPS and GSM based engine locking system using smart password. *International Journal of Computer Sciences and Engineering, 5*(4), 57-61. Retrieved from http://www.ijcseonline.org/pub-paper/10-IJCSE-02023.pdf

Park, B., & DeMarco, C.L. (2016). Optimal controls via waveform relaxation for power systems cyber-security applications. *2016 IEEE Power and Energy, Society General Meeting (PESGM)*. doi:10.1109/PESGM.2016.7741585

Rossi, B. (2016, February 3). 7 steps hackers take to execute a successful cyber attack. Retrieved from https://www.information-age.com/7-steps-hackers-take-execute-successful-cyber-attack-123460872/

Rubin, S.H., Grefe, W.K., Bouabana-Tebibel, T. Chen, S., Shyu, M., & Simonsen, K.S. (2017). Cyber-secure UAV communications using neuristically inferred stochastic grammars and hard real-time adaptive waveform synthesis and evolution. In *2017 IEEE International Conference on Information Reuse and Integration (IRI)*. Retrieved from https://users.cs.fiu.edu/~chens/PDF/IRI17_stuart.pdf

Shin, H., Son, Y., Park, Y.S., Kwon, Y., & Kim, Y. (2016). Sampling race: Bypassing timing-based analog active sensor spoofing detection on analog-digital systems. Retrieved from https://www.usenix.org/system/files/conference/woot16/woot16-paper-shin.pdf

Shipley, A.J. (2013, June 19). Operating system hardening techniques and security strategies. Retrieved from http://blogs.windriver.com/wind_river_blog/2013/06/operating-system-hardening-techniques-and-security-strategies.html

Shoukry, Y., Nuzzo, P., Puggelli, A., Sangiovanni-Vincentelli, A.L., Seshia, S.A., & Tabuada, P. (2017). Secure state estimation for cyber-physical systems under sensor attacks: A satisfiability modulo theory approach. *IEEE Transactions on Automatic Control, 62*(10), 4917-4932. Retrieved from https://arxiv.org/pdf/1412.4324.pdf

Sigg, S. (2011, January 31). Operating systems: Security and protection. Retrieved from http://www.stephensigg.de/stephen/Lectures/OS/OperatingSystems-Ws10_Slides-07_SecurityProtection_101020_v1.0_STS.pdf

Six, J. (2012). Application security for the android platform. North Sebastopol, CA: O'Reilly Media, Inc.

Smith, D.A. (2017, September 13). 7 steps of a cyber attack and what you can do to protect your windows privileged accounts. Retrieved from https://beyondtrust.com/blog/7-steps-cyber-attack-can-protect-windows-privileged-accounts/

Son, Y., Shin, H., Kim, D., Park, Y.S., Noh, J., Choi, K., Choi, J., & Kim, Y. (2015, August 12-14). Rocking drones with intentional sound noise on gyroscopic sensors. *Symposium conducted at the Proceedings of the 24th USENIX Security Symposium* in Washington, D.C. Retrieved from https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-son.pdf

Verma, A. (n.d.). Securing automotive software over the air updates. Retrieved from https://excelfore.com/blog/securing-automotive-software-air-updates/

Weber, M. (2014, May 8). Where to? A history of autonomous vehicles. Retrieved from https://www.computerhistory.org/atchm/where-to-a-history-of-autonomous-vehicles/

Yan, C., Xu, W., & Liu, J. (2016). Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle. *DefCON 24*, 24. doi:10.1145/1235. Retrieved from https://www.co.tt/files/defcon24/Speaker%20Materials/DEFCON-24-Liu-Yan-Xu-Can-You-Trust-Autonomous-Vehicles-WP.pdf

## About the Authors

### Charles Parker II, PhD

Charles Parker has over a decade of experience in the InfoSec industry beginning in the banking industry and continuing through the medical and vehicle industries. He focused on improving InfoSe environment through presenting on various subjects, writing extensively on cybersecurity Application and breaches and consulting. He holds an MBA, MSA, JD, LLM, and PhD.

### Nikolas Upton

Nikolas Upton has been conducting security research since 2011. Most of the time has been spent confirming the methodology and utility of different attack methods. Recent years have been spent applying this knowledge to secure autonomous cars and OEM parts.

# Writing Skills and Challenges for
# Engineering Technology Students

Dr. Anne Lucietto
Purdue University, Purdue Polytechnic Institute

Dr. Nichole Ramirez
Purdue University, Purdue Polytechnic Institute

## Abstract

This paper explores how engineering technology students share their thoughts and logical processes through written communication. It is particularly important to assess the ability of these students as they convey their thoughts and technical judgment. Professors and potential employers find engineering technology students to be technically competent but lacking in communication skills. The researchers are particularly interested in writing skills, as this appears to be one of the skills that students lack as they transition into their post-graduate careers. This work is intended to provide a venue to encourage better writing skills in all students, and to increase the understanding of engineering technology students through an examination of the content of their technical writing product. It also provides a further understanding of how practitioners can encourage the improvement of writing skills of engineering technology students.

*Keywords:* engineering technology students, communication skills

## Introduction

This study is based on a writing assignment designed for a fluid mechanics course and referred to as the “Big Question Reflection.” The authors are involved in teaching and researching engineering technology students. It is the researchers intent to help the engineering technology students because this engineering technology student population is noted by employers as lacking in basic communication skills, in particular writing (Hart Research Associates, 2015; National Association of Colleges and Employers, 2016). Furthermore, the field of engineering technology  is often viewed through the lens of other Science, Technology, Engineering, and Mathematics (STEM) research (Freeman et al., 2014; Goldstein, 2016). When studies combine student populations or make assumptions that all students are alike or at least similar, those things that should be known about a given student population are obscured (Anne M. Lucietto, Moss, Efendy, & French, 2017). Work to develop an understanding of a unique group of students is important in the development of tools and means to educate and prepare engineering technology students for the workplace.

## Literature Review

Studies such as one done by Hart Associates (2015) and others (National Association of Colleges and Employers, 2016; Stewart, Wall, & Marciniec, 2016) indicate that employers are disappointed in the student's lack of communication skills, most notably writing (National Association of Colleges and Employers, 2016). Unfortunately, practitioners, industrial representatives, and others have noticed the lack of writing skills for quite some time. The lack of these skills continues to be noted (Bazerman, 2005; Russell, 1990). Through this work, it is becoming clear that it is imperative that well-crafted assignments be used throughout the program curricula to provide the practice necessary to improve writing skills throughout students' time in the program. Faculty involved in this research have addressed this issue by developing an assignment which consists of a compilation of assignments, a collection of tools that will enable and improve students' writing skills throughout the semester. The intent of this work is to improve writing skills in all students, while evaluating the change in writing skills throughout the semester and between student groups, and to better understand engineering technology students.

Several organizations have produced reports that support the fact that technical personnel in the STEM fields need to be skilled in communication (Hart Research Associates, 2015). They also assert that they should be creative (Kuhn, Greenhalgh, & McDermott, 2016) and able to function in a multifaceted environment (Scharf, 2014). Engineering technology graduates, as well as those in other STEM fields, must develop competencies in research, critical analysis, and the synthesis of information to provide clients and customers with a final project that meets their technical needs (Wertz, Ross, Fosmire, Cardella, & Purzer, 2011). Unfortunately, researchers have found that many STEM graduates do not possess the communication skills needed and desired by their employers (Archer & Davison, 2008; Hart Research Associates, 2015). Potentially, a future area to research may include learning more about how ABET's (ABET Technology Accreditation Commission, 2009) criteria for engineering technology programs in communication skills is successfully addressed.

### Skill Development

Students that enroll into engineering technology programs generally have higher SAT scores, which usually are a combination of high SAT Math scores with lower SAT Verbal scores. This is true of most students in STEM fields (Anne M. Lucietto, 2014). Due to the aggregated data with other STEM fields, engineering technology student data often becomes obscured by engineering and the other fields in STEM, making delineation of engineering technology students as a separate population difficult. Based upon current literature, it appears that the development of writing skills within this and other STEM student bodies is a difficult concept to enact throughout curriculums and institutions (Bicer, Capraro, & Capraro, 2013; Cappelli, 2014). If academics were queried, they would agree that writing skills are important and should be practiced (Kamler & Thomson, 2014; Street, 2015). Many researchers state that the university is responsible for assuring students have, gained, and maintain quality writing skills (Chittum & Bryant, 2014; Weissbach & Pflueger, 2014). However, other factors complicate and confound success in such an endeavor. These include faculty pushback, based upon the increased workload for faculty whose specialty is something other than literature and writing (Hillyard, 2012). While faculty are expected to write, their skills are often different than those that are desired for a program such as "writing across the curriculum"(Arum & Roksa, 2011). The English department at various institutions may be concerned with skills developed by faculty whose specialty is not in English when the teaching occurs outside of the venue of a traditional English course (Condon & Rutz, 2012). Finally, most STEM students are required to take freshman English courses and, in some cases, a technical writing skills incorporated through writing assignments included in coursework during the last two years of their studies. Without opportunities to practice the skills gained in these courses, students are unable to maintain and enhance their writing skills (Soliday, 2011).

## Improve Writing Skills

More and more institutions have formalized the "writing across the curriculum" concept with the intent of increasing the student's opportunity to practice writing. However, the challenges met by these programs have been perplexing (Hillyard, 2012). Maki (2012) asserts that to achieve and sustain success in a program of this type support from the top of the organization is essential. Earlier work shows that communication skills both in the spoken and written language are critical for success in a student's career (Israel & de Jager, 2009). Many graduates of engineering technology programs have realized that it is imperative to share their ideas, technical content of projects, and other work with their peers, superiors, subordinates, and clients (Haik, Sivaloganathan, & Shahin, 2015; Rajendran, Kannan, Sathish, & Durgadevi, 2016; Spence & Liu, 2013). Rather than acquiring these skills in the classroom, well before entering the workplace, they are developed on the job. Graduates are finding that the development of these skills should be done prior to entering the workforce and should be gained in the classroom, through both formal and informal writing assignments, presentations, and general discussion (Bell, 2009).

Engineering technology faculty, while they may write scholarly articles as a result of their research, are generally not formally educated in teaching communication skills in the classroom (Goldstein, 2016). This is where English faculty are concerned with the execution of "writing across the curriculum" assessments. Primarily their concern is the inconsistency between faculty members and the potential of bias due to familiarity with the students (Israel & de Jager, 2009). This point is argued frequently, but most of the faculty with this opinion support the notion that the best way to encourage learning is through writing (Bangert-Drowns, Hurley, & Wilkinson, 2004; Bean, 2011; Klein & Yu, 2013; Mayer, 2013; Oatley & Djikic, 2008; Ong, 2012; Wadsworth, 1996). The concept of writing to learn has not been studied much at this level of education. Only a few researchers have investigated this area of study (Klein & Yu, 2013; Reynolds, Thaiss, Katkin, & Thompson, 2012; Waters, 2014). Therefore, observing what the students do throughout their studies, or in the individual classroom, provides a better understanding of what improves the students' writing skills and how to achieve that goal.

### Increase Understanding of Engineering Technology Student

Writing to learn is a technique used by teachers to provide writing assignments with the intent of helping them understand the material they are studying (Bangert-Drowns et al., 2004; Kamler & Thomson, 2014; Klein & Yu, 2013; Reynolds et al., 2012). This assignment type is intended to aid the student in better understanding course concepts by engaging in both formal and informal learning (Bangert-Drowns et al., 2004; Bell, 2009; Klein & Yu, 2013). When using the writing to learn technique for conceptual learning, assignments must be crafted carefully with a review of best practices.

Researchers discussing how students learn fluids, thermodynamics, and similar material agreed that when students engage in the material they generally have a positive experience (Hamari et al., 2016; Reeve & Lee, 2014). Further debate on the subject included methodologies that could be used to engage the students in course material in such a way that they search out more to help them in their understanding of that which is relative to their interests (Beetham & Sharpe, 2013; Prince, 2004). This leads to further investigation regarding how students learn, and how to develop an assignment that engages and provides an opportunity to expand students' knowledge into the course material, as well as outside of it.

## Research Questions

Using the available writing assignments and considering the statements made by employers, the researchers ask the following questions:

- Does the assignment developed and discussed in this paper provide a venue for writing skill development?
- Does this assignment provide a means for practitioners to encourage the improvement of writing skills of the engineering technology student?
- Does this assignment provide a means to increase our understanding of engineering technology students through content analysis of the technical writing product?

## Methods

To answer the three research questions posed by the researchers, the documents prepared by the students must be examined using a couple of techniques. First, there is a review of the assignment and student writing skills, then there is an analysis of students' writing skills to determine if there was an improvement from the first to the last writing assignment in the project. Finally, there is a review to determine what we can learn about the engineering technology student using content analysis as the tool to review the writing product.

### Review of Assignment – Writing Skills

The development of the assignment initially considered previous assignments and data found in a resource "Engaging Ideas" (Bean, 2011). The course instructor, who is also the first author, modified a reflection assignment used in previous classes and created the "Big Question Reflection,"(A.M. Lucietto & Ramirez, 2015) or BQR as the students refer to it.

The assignment is part of a fluid mechanics course where the students are usually within a semester or two of graduating. However, the assignment was designed with the intention of portability across topics and majors. It is open ended, which provides a forum for students to choose their own topic and perform passive and active research, because of concepts used in other courses (Bean, 2011; Emig, 1994; Mayer, 2013; Oatley & Djikic, 2008). The assignment is based upon constructivist theory (Piaget & Vygotsky's, 1969; Vygotsky, 1978), in particular student-centered learning (Lee & Hannafin, 2016), using scaffolded techniques (Jackson, Krajcik, & Soloway, 1998; Trif, 2015) to build student knowledge and understanding while motivating (Lompscher, 1999; Manning, 2011) them to engage in material that is required and not easily engaged (Kim, Park, Huynh, & Schuermann, 2017). This is particularly important as students at this time in their studies experience a phenomena called "senioritis" and often disengage prior to the end of this period of learning (Magruder & Degges-White, 2013; Manning, 2011). Utilizing scaffolded learning techniques (Quarles, Lampotang, Fischler, Fishwick, & Lok, 2009), and a constructivist approach (Trif, 2015; Wadsworth, 1996) the author built the assignment for two reasons: the first to encourage writing and development of thought (Goss, 2017) as it relates to something that interests the student and second to utilize things that the author used during the years she spent in industry in the development and completion of projects. The assignment that was developed follows:

> Part 1 – The Big Question
> What would you like to learn in MET 313? Have you thought about the things we will cover and may discuss in the course? Review your text and material related to the concepts covered in this course. Write a question and justify your reasoning behind your particular question and submit it for approval.

Part 2 – Passive Research
This submission should include your notes, thoughts, and findings related to your answer of your initial approved question. You should have passive research (book, library, online searching). You also are expected to provide a description of how you will proceed with your active research (calling vendors, talking to other professors, etc.).

Part 3 – Active Research
This submission should include your notes and thoughts, as well as your findings while doing active research (calling vendors, talking to other professors, etc.).

Part 4 – Final Submission and Presentation
You are required to submit a final reflection on what you learned. Share the answer to your question and include your thoughts regarding how this assignment impacted you and helped your learning.

Students became engaged in the material and began searching for new and innovative materials, while in the final assignment they wrote a summary of the answer to their question, a reflection of the work done, and things learned. Students receive feedback after submitting each of the four parts of the paper.

**Improvement in Writing Skills throughout the Semester**

Based upon previously presented evidence, and practice, the researchers studied the content and reading ease of the first and last assignment. In published work the authors found that the four assignments that required students to write, edit, and understand a subject of personal interest did improve students' writing skills over the semester (A.M. Lucietto & Ramirez, 2015). The authors have included a comparison in order to review the newer data.

**Learning About Engineering Technology Students**

To learn more about the engineering technology students (participants) their level of study, anticipated graduation was examined, while the content (content analysis) of the students writing and reflection was examined to further understand these students and their understanding of the subject matter.

Participants. Engineering technology students whose writing was examined for this study were in the same year, but generally were graduating following the fall or spring semester. Over 95% of these students in each class graduated following the semester they were in this course. There were two Cohorts of students identified, with Cohort 1 being students from the Fall semester and Cohort 2 from the Spring semester. Students varied a little with the majority of students traditional and in their fourth year of study in the program. Most graduated within a semester of completing this course.

Content Analysis. Using content analysis, the authors show how writing assignments can elicit students' understanding of course concepts. Content analysis usually results in two areas of observation within the data. The first is reviewing the content of the items being studied and developing inferences about what is written and the second is counting frequencies of symbols (de Sola Pool, 1959). Others refer to this first methodology as qualitative content analysis (Schreier, 2012), which is defined as systemic analysis that results in answers generated by the nature of the data.

Schreier (2012) clarifies content analysis by defining it as three-fold. The components of qualitative content analysis are systematic method, flexible method, and a means to reduce the data for interpretation. The first, systematic method, has a sequence of eight steps, which includes deciding the question; choosing the data; developing coding or a means to divide the data, if needed; modification of the coding; analysis; and disseminating the findings. Flexible is used to define content analysis by suggesting that coding or means to divide the data is designed for the data or material being analyzed. Finally, the reduction of data that is contrary to most other methods aids the summarization and interpretation of the qualitative data.

Review of technical content practices by Andersen (2014) reveals that decisions and interpretation of technical content is often based on intuitive practices rather than the data itself. She finds that the practices used in documentation of technical content are based on tradition rather than research. Thus, the authors have chosen content analysis to provide a better understanding of engineering technology students, with the intent of determining if this is a venue to aide in writing skill development, provide practitioners with a means to improve writing skills in engineering technology students, and to further our understanding of engineering technology students via analysis of this technical writing product.

## Results

The analysis of the materials provided by students in Cohort 1 and 2 provide a different perspective. Based upon the research questions, the following findings show what the authors found in relationship to each.

## Review of Assignment – Writing Skills

Initial analysis included an extraction of technical terms noted on the course syllabus, with particular attention given to course objectives. This allowed the researchers to compare students' responses with course content. Reviewing the reflective assignments, weighted percentages were calculated by dividing the number of occurrences of each term by the total number of words in the assignment, excluding connecting words and pronouns. The researchers used weighted percentages to account for variances in the length of students' responses. The weighted percentages of the top ten terms emerged and are noted in descending order in Table 1. The most common terms aligned with the course syllabus and objectives, suggesting that the assignment was an effective vehicle for students to generate and communicate their course-related research ideas.

Table 1. Top ten terms from weighted percentages over all cohorts.

| |
|---|
| engine |
| systems |
| pressure |
| flow |
| power |
| hydraulic |
| viscosity |
| compressor or compress |
| turbulent |

Cohort 1 and 2 were studied, taking the same course one semester after another, and working on the same assignment, with the same instructions and instructor. After summing the weighted percentages of each term in all assignments, 40 terms emerged. The largest gap was between the tenth and eleventh terms, resulting in a list of 10 terms each, with a weighted percentage above 10%. One unique case was the term "pump." Every student in the first cohort studied mentioned pump at least once in the first or fourth assignment. When comparing the terms, it was noted that the first cohort also exhibited the only two decreases in technical terms between the initial and final assignment (Students A and E). Additionally, the second cohort of students consistently had a greater increase in the number of terms compared to their peers. The assignment was not changed. It was presented in the same perspective to the students and followed up similarly in both semesters. In general, students understand the project from conversations with others. However, they are required to choose a project that has meaning to them and is independent of others in the course. Many of the words are similar but are related to the course material that focuses on pumps, fluid flow, and other related terms. The independent nature of the assignment prevents sharing of information or any cooperative efforts that may impinge on the nature of student output.

**Improvement in Writing Skills throughout the Semester**

Table 2 is an exhibit of the number of unique technical terms in each assignment. The difference column represents the increase or decrease in the number of terms between the initial and final assignments. The first column showing students A through J shows each student randomly chosen for analysis in each cohort.

Table 2. Number of unique technical terms in each assignment.

| | Student | Initial | Final | Difference |
|---|---|---|---|---|
| Cohort 1 | A | 9 | 3 | -6 |
| | B | 10 | 10 | 0 |
| | C | 9 | 16 | 7 |
| | D | 14 | 14 | 0 |
| | E | 8 | 7 | -1 |
| Cohort 2 | F | 11 | 16 | 5 |
| | G | 6 | 8 | 2 |
| | H | 5 | 18 | 13 |
| | I | 9 | 16 | 7 |
| | J | 14 | 18 | 4 |

**Learning About Engineering Technology Students**

Table 3 includes the weighted percentage of all technical terms in each assignment. Most students' final assignments contained lowered weighted percentages of technical terms than the initial. Student G was the only example of an increase in weighted percentage in Cohort 2. After review, one explanation for this may be the length of the assignment. As the length of the essay increases, the weighted percentage of individual terms usually decreases.

Table 3. Weighted percentage of total technical terms in each assignment.

| | Student | Initial | Final | Difference |
|---|---|---|---|---|
| Cohort 1 | A | 14.9 | 7.6 | -7.3 |
| | B | 12 | 14.3 | 2.3 |
| | C | 8.4 | 7.5 | -0.9 |
| | D | 17.1 | 18.5 | 1.4 |
| | E | 7.1 | 7.1 | 0 |
| Cohort 2 | F | 24.5 | 13.4 | -11.1 |
| | G | 9.4 | 12 | 2.6 |
| | H | 12.5 | 10.4 | -2.1 |

| | | | |
|---|---|---|---|
| I | 21.7 | 14.3 | -7.4 |
| J | 9.4 | 9.1 | -0.3 |

The overall increase in the unique number of technical terms shows that students have a broader understanding of the course topics. However, the decrease in weighted percentages of technical terms may also be indicative of a shift toward more reflective language as the assignment asks students to share their thoughts on how the assignment influenced them and helped them learn. This demonstrates that students developed a broader understanding of the course material, and through their reflections have expressed higher-level thinking.

## Conclusions

Using content analysis, the data analysis included evaluation of essays submitted as part of the BQR. Various technical terms were identified using content analysis. Then, terms were counted and weighted percentages were calculated. The qualitative method was conducive to further quantitative analysis, thus resulting in a mixed methods study.

Previously a study completed on Cohort 1 (A.M. Lucietto & Ramirez, 2015) compared the first and last assignments of this project. Each of the assignments from the randomly chosen students was examined for unique technical terms. Comparison of the first and last assignments focuses on the change in the number of technical terms used in the essays. The difference column shows that two students decreased the number of technical terms used in the first and last assignment, while most showed an increase. This study focused on using those methods that were most beneficial to understanding the engineering technology students. Continuing to use the data from five randomly chosen students in the two cohorts that had the same assignment, quantitative methods measured the difference in the number of technical terms in the first and last assignment. The focus was three-fold, with the first concentrating on the top terms using weighted percentages, then unique technical terms from first to last essay, and a weighted percentage of total technical terms in each assignment.

The majority of these terms were found on the syllabus, indicating that the project direction was accordant with the materials presented in the course. The essays submitted for the first and last piece of this assignment showed that students in Cohort 2 used more technical terms in the last essay than Cohort 1. Students in Cohort 1 were the first to do the BQR in this particular course offering and students in this program always share course information with one another. The instructor, when referring to the assignments, stressed use of technical terminology. It appears that Cohort 2 may have absorbed that much more than Cohort 1.

Using a weighted percentage, comparing the first and last assignment of each student shows a difference in the use of technical terms overall by each cohort. More students in Cohort 2 had a negative difference in weighted percentage than Cohort 1. The course offered in Fall and Spring semesters, with Cohort 1 being Fall and Cohort 2 being Spring, potentially explaining why there are distinct differences between cohorts.

Evaluation of reflection and writing output, from a humanities standpoint in literature, is prevalent (Kori, Pedaste, Leijen, & Mäeots, 2014), but literature from the technical stand point is not as palpable. Therefore, literature focused on the quality of student reflection (Leijen, Valtna, Leijen, & Pedaste, 2012) in the humanities was reviewed and used to inform the qualitative method of evaluation.  Further appraisal using evaluation of phrasing, combination of wording, and overall essay evaluation for technical relevance as well as alignment with the course materials were completed. The result supported that the words, in context, and relevant to both the BQR topic and course material, confirming that the evaluation methods provided a consensus regarding the quality of technical reflection achieved.

While the investigators did not use triangulation in the traditional sense (Denzin, 1970), the three different methods of evaluation, quantitative, qualitative, and essay review, show that the findings from each method align. Results support the quantitative findings and lead to the third aspect of this analysis that includes investigator review, and review of essays.

Due to the open nature (de Vries, Grond, & van der Zee, 2015) of the assignment, students are often initially frustrated and become exasperated with developing their initial question.  The open-ended nature of the assignment also increases the workload of the instructors, as they need to identify the frustrated students and make sure all of the questions complement the course materials.

This assignment requires careful review of content, composition, and the writing students use to communicate throughout the course. The essence of the assignment is technical, but also relies on soft skills by requiring students to reflect (Tollefson, Francis, & Usher, 2001). Methods to analyze this type of work, particularly to evaluate the change in verbiage, and skill improvement, are focused on one area of study or a small combination of topics. Review of the various methodologies lead the authors to Content Analysis, which is used in a large variety of topics, and divergences in the skills needed to study them (Krippendorff, 2012). This thus provides an understanding of the development of this assignment, demonstration of engagement in the course material, and the success of this particular assignment in the development of technical writing skills.

Students completing the Big Question Reflection assignment appeared to develop their projects and final discussions in a manner that was wholly reflective of terms related to the course. With these terms, regardless of the semester being analyzed, the investigators found that students used more technical terms in the final assignment. Using terms that are more technical resulted in a decrease in the weighted percentage. In some cases, students did not include more course topics in their final assignment and the weighted percentage of technical terms decreased, implying that those students are using other language. The analysis revealed a gap in students' language that may indicate a shift toward reflective language in the final assignment. If so, students' submissions align with the descriptions of the initial and final assignment, the Big Question Reflection. The findings can be useful for educators to adapt curricula and assignments to align with course objectives.

While performing the analysis of technical language, the authors found that an analysis of reflective terms that are rich in information will provide enlightenment on attitude, judgement, and appreciation of the topic. The analysis of this study revealed an unexplored aspect of engineering technology writing – reflective language. Further exploration of this aspect of engineering technology students' writing may clarify the identity, and critical thinking skills of this population.

## References

ABET Technology Accreditation Commission. (2009). Criteria for Accrediting Engineering Technology Programs. In: October.

Andersen, R. (2014). Rhetorical work in the age of content management: Implications for the field of technical communication. Journal of Business and Technical Communication, 28(2), 115-157.

Archer, W., & Davison, J. (2008). Graduate employability. The council for industry and Higher Education.

Arum, R., & Roksa, J. (2011). Academically adrift: Limited learning on college campuses: University of Chicago Press.

Bangert-Drowns, R. L., Hurley, M. M., & Wilkinson, B. (2004). The Effects of School-Based Writing-to-Learn Interventions on Academic Achievement: A Meta-Analysis. Review of Educational Research, 74(1), 29-58. doi:10.3102/00346543074001029

Bazerman, C. (2005). Reference guide to writing across the curriculum: Parlor Press LLC.

Bean, J. C. (2011). Engaging ideas: The professor's guide to integrating writing, critical thinking, and active learning in the classroom: John Wiley & Sons.

Beetham, H., & Sharpe, R. (2013). Rethinking pedagogy for a digital age: Designing for 21st century learning: routledge.

Bell, P., Ed., Lewenstein, Bruce, Ed., Shouse, Andrew W., Ed., & Feder, Michael A., Ed. (2009). Learning Science in Informal Environments: People, Places, and Pursuits. . Washington, DC.

Bicer, A., Capraro, R. M., & Capraro, M. M. (2013). Integrating writing into mathematics classroom to increase students’ problem solving skills. International Online Journal of Educational Sciences, 5(2), 361-369.

Cappelli, P. (2014). Skill gaps, skill shortages and skill mismatches: evidence for the US. Retrieved from

Chittum, J. R., & Bryant, L. H. (2014). Reviewing to Learn: Graduate Student Participation in the Professional Peer-Review Process to Improve Academic Writing Skills. International Journal of Teaching and Learning in Higher Education, 26(3), 473-484.

Condon, W., & Rutz, C. (2012). A taxonomy of writing across the curriculum programs: Evolving to serve broader agendas. College Composition and Communication, 64(2), 357-382.

de Sola Pool, I. (1959). Trends in Content Analysis. Eidted by Ithiel de Sola Pool: University of Illinois Press.

de Vries, B., Grond, M., & van der Zee, A. (2015). Development of a multi-disciplinary university wide design course.

Denzin, N. (1970). Strategies of multiple triangulation. The research act in sociology: A theoretical introduction to sociological method, 297, 313.

Emig, J. (1994). Writing as a Mode of Learning. Landmark Essays on Writing Across the Curriculum, 89-96.

Freeman, S., Eddy, S. L., McDonough, M., Smith, M. K., Okoroafor, N., Jordt, H., & Wenderoth, M. P. (2014). Active learning increases student performance in science, engineering, and mathematics. Proceedings of the National Academy of Sciences, 111(23), 8410-8415.

Goldstein, J. E. (2016). Assessing Students' Writing: Countering Some Common Misbeliefs.

Goss, D. A. (2017). Using Writing Assignments to Improve Student Engagement and Learning. Optometric Education, 42(2), 2016.

Haik, Y., Sivaloganathan, S., & Shahin, T. M. (2015). Engineering design process: Cengage Learning.

Hamari, J., Shernoff, D. J., Rowe, E., Coller, B., Asbell-Clarke, J., & Edwards, T. (2016). Challenging games help students learn: An empirical study on engagement, flow and immersion in game-based learning. Computers in Human Behavior, 54, 170-179.

Hart Research Associates. (2015). Falling Short? College Learning and Career Success. Retrieved from

Hillyard, C. (2012). Comparative Study of the Numeracy Education and Writing Across the Curriculum Movements: Ideas for Future Growth. Numeracy, 5(2), 2.

Israel, H. F., & de Jager, H. J. (2009, 23-25 Sept. 2009). Assessing the written word: The engineering students' experience. Paper presented at the AFRICON, 2009. AFRICON '09.

Jackson, S. L., Krajcik, J., & Soloway, E. (1998). The design of guided learner-adaptable scaffolding in interactive learning environments. Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Los Angeles, California, USA.

Kamler, B., & Thomson, P. (2014). Helping doctoral students write: Pedagogies for supervision: Routledge.

Kim, C., Park, S. W., Huynh, N., & Schuermann, R. T. (2017). University students' motivation, engagement and performance in a large lecture-format general education course. Journal of Further and Higher Education, 41(2), 201-214.

Klein, P. D., & Yu, A. (2013). Best practices in writing to learn. Best practices in writing to learn (2nd ed.), The Guilford Press, New York, 166-189.

Kori, K., Pedaste, M., Leijen, Ä., & Mäeots, M. (2014). Supporting reflection in technology-enhanced learning. Educational Research Review, 11, 45-55.

Krippendorff, K. (2012). Content analysis: An introduction to its methodology: Sage.

Kuhn, M. A., Greenhalgh, S., & McDermott, M. (2016). Using Creativity from Art and Engineering to Engage Students in Science. Journal of STEM Arts, Crafts, and Constructions, 1(2), 2.

Lee, E., & Hannafin, M. J. (2016). A design framework for enhancing engagement in student-centered learning: own it, learn it, and share it. Educational Technology Research and Development, 64(4), 707-734.

Leijen, Ä., Valtna, K., Leijen, D. A., & Pedaste, M. (2012). How to determine the quality of students' reflections? Studies in Higher Education, 37(2), 203-217.

Lompscher, J. (1999). Motivation and activity. European Journal of psychology of education, 14(1), 11-22.

Lucietto, A. M. (2014). The Role of Academic Ability in Choice of Major and Persistence in STEM Fields. (Ph.D.), Purdue University, West Lafayette, IN.

Lucietto, A. M., Moss, J. D., Efendy, E., & French, R. M. (2017). Engineering Technology vs Engineering Students Differences in Perception and Understanding. Paper presented at the FIE Frontiers in Education Annual Conference, Indianapolis, IN.

Lucietto, A. M., & Ramirez, N. (2015). Writing Proficiency in Engineering Technology Students and Skill Development in the Classroom Paper presented at the ASEE Annual Conference and Exposition, Seattle, Washington.

Magruder, J., & Degges-White, S. (2013). Counseling Concerns Over the College Academic Year. College Student Mental Health Counseling: A Developmental Approach, 13.

Maki, P. L. (2012). Assessing for learning: Building a sustainable commitment across the institution: Stylus Publishing, LLC.

Manning, C. (2011). "Senioritis:" An Analysis of Academic Motivation and Burnout in College Students through the Lens of Positive Psychology.

Mayer, R. (2013). How engineers learn: a study of problem-based learning in the engineering classroom and implications for course design.

National Association of Colleges and Employers. (2016). Job Outlook 2016: Attributes Employers Want to See on New College Graduates' Resumes. Retrieved from http://www.naceweb.org/s11182015/employers-look-for-in-new-hires.aspx

Oatley, K., & Djikic, M. (2008). Writing as thinking. Review of General Psychology, 12(1), 9.

Ong, W. J. (2012). Orality and literacy: The technologizing of the word: Routledge.

Piaget, J., & Vygotsky's, L. (1969). The theories of cognitive development. In: New York: McGraw-Hill.

Prince, M. (2004). Does active learning work? A review of the research. Journal of Engineering Education, 93(3), 223-231.

Quarles, J., Lampotang, S., Fischler, I., Fishwick, P., & Lok, B. (2009). Scaffolded learning with mixed reality. Computers & Graphics, 33(1), 34-46.

Rajendran, M., Kannan, T. R., Sathish, V., & Durgadevi, M. (2016). The Relevance of Communication Skills to the Technical Students in the Colleges of Engineering and Technology-A Study. Indian Journal of Science and Technology, 9(19).

Reeve, J., & Lee, W. (2014). Students' classroom engagement produces longitudinal changes in classroom motivation. Journal of Educational Psychology, 106(2), 527.

Reynolds, J. A., Thaiss, C., Katkin, W., & Thompson, R. J. (2012). Writing-to-learn in undergraduate science education: A community-based, conceptually driven approach. CBE-Life Sciences Education, 11(1), 17-25.

Russell, D. R. (1990). Writing across the curriculum in historical perspective: Toward a social interpretation. College English, 52-73.

Scharf, D. (2014). Instruction and assessment of information literacy among STEM majors. Paper presented at the Integrated STEM Education Conference (ISEC), 2014 IEEE.

Schreier, M. (2012). Qualitative content analysis in practice: Sage Publications.

Soliday, M. (2011). Everyday genres: Writing assignments across the disciplines: SIU Press.

Spence, P., & Liu, G.-Z. (2013). Engineering English and the high-tech industry: A case study of an English needs analysis of process integration engineers at a semiconductor manufacturing company in Taiwan. English for specific purposes, 32(2), 97-109.

Stewart, C., Wall, A., & Marciniec, S. (2016). Mixed Signals: Do College Graduates Have the Soft Skills That Employers Want? Paper presented at the Competition Forum.

Street, B. V. (2015). Academic Writing: Theory and Practice. Journal of Educational Issues, 1(2), 110-116.

Tollefson, J., Francis, D., & Usher, K. (2001). Moving from technical to critical reflection in journalling: an investigation of students' ability to incorporate three levels of reflective writing.

Trif, L. (2015). Training Models of Social Constructivism. Teaching Based on Developing A Scaffold. Procedia-Social and Behavioral Sciences, 180, 978-983.

Vygotsky, L. (1978). Interaction between learning and development. Readings on the development of children, 23(3), 34-41.

Wadsworth, B. J. (1996). Piaget's theory of cognitive and affective development: Foundations of constructivism: Longman Publishing.

Waters, P. M. (2014). Writing to Learn. Perspectives (TESOL Arabia), 22(1).

Weissbach, R., & Pflueger, R. (2014). Technical writing knowledge transfer from first year composition to major courses. Paper presented at the Frontiers in Education Conference (FIE), 2014 IEEE.

Wertz, R. E., Ross, M., Fosmire, M., Cardella, M., & Purzer, S. (2011). Do students gather information to inform design decisions? Assessment with an authentic design task in first-year engineering.

## About the Authors

### Anne Lucietto, PhD

Dr. Anne Lucietto has nearly three decades of progressively responsible experience in industry, paired with adjunct teaching experience, and now as a full-time engineering technology faculty member. She has worked in a variety of industries such as power generation, fasteners, and heavy machinery; she has managed construction projects in national laboratories and for start-up projects. She researches her primarily senior students and is finding that the transition out of the classroom and into the career is something to learn more about. Dr. Lucietto has focused on researching students that are women and minorities, considering problems specifically encountered by this research population.

### Nichole Ramirez, PhD

Dr. Nichole M. Ramirez is the Assistant Director of the Vertically Integrated Projects (VIP) program in the College of Engineering at Purdue University. Previously, Nichole was a Research Data Analyst in the Office of Institutional Research, Assessment and Effectiveness at Purdue University and the Associate Director for Policy Analysis for the Multiple-Institution Database for Investigating Engineering Longitudinal Development. Her work focuses on student persistence and outcomes in engineering, engineering technology, and cooperative education, disaggregating by gender, race/ethnicity, and socioeconomic status. She received her PhD in Engineering Education and M.S. in Aviation and Aerospace Management from Purdue University.

# APPEAL FOR EQUILIBRIUM:
# Unbalanced Culture of Women and Minorities in Cybersecurity Domain

Dr. Joseph O. Esin
Professor of Computer Information Systems/Cybersecurity
Jarvis Christian College, Hawkins, Texas USA
Visiting Professor of Research, University of Calabar, Nigeria

## Abstract

Traditionally there has been fewer women and racial minorities in the cybersecurity domain. Despite the fact that there is an ever-increasing number of unfilled positions in cybersecurity, this trend has not changed. An unbalance still exists. This article presents a framework, discusses some of the women and minority talent that exists and presents the need to eradicate this issue.

*Keywords: Women, minorities, cybersecurity, culture*

## Preamble

Culture is made up of the customs, beliefs and rules of society. It is a general believe that men are a more assertive, self-assured and formidable group while women are less confident, undecided, noncommittal by nature, and unfit in the cybersecurity domain ((Esin, 2018; Hu, 2014; & Elan, 2012). As LeClair & Pheils (2016) and Esin, (2019) noted, despite gender stereotyping and culturally bias beliefs in the inferiority of women in the domain of cybersecurity, it is worth noting that women and minorities continue to aspire as unwavering contributors in the battle against cyber-attacks and cyber-threats on the vulnerable innocent citizens. The development of computer system after the Second World War witnessed less than adequate participation of women and racial minorities in cybersecurity. The retention of the few women and minorities who embraced cybersecurity careers remains at a dismal low level revealing that most of these women and minorities lag in pursuing a cybersecurity career. It is time to revisit the overstretched cybersecurity career policy, re-engage women and minorities based on their intellectual capability not on corporeal competence (Ngwang, 2018 and Esin, 2019). To eradicate the looming inequalities, it is critical to envisage and engage an intelligence mitigation plan of action aimed at dismantling the baggage of gender stereotyping, which has hitherto suppressed talented women and minorities. Undergirding this initiative should be the overwhelming determination to ensure that the recruitment policy for cybersecurity professionals is organized to include women and minorities. From a religious view of **creation, the male concept of the leadership role of men created a common ground for** systemic men dominance in all aspects of life including the cybersecurity profession. However, human evolution has revealed that women can do as much of everything men do, if not better. As a result, today, men are strongly encouraged to accept professional alliance with their women and minority compatriots as partners who complement each other's roles and responsibilities.

## Framework

Per (Tsai, 2016) and (Hu, 2014), participation of women and minorities in cybersecurity workforce remains unbalanced in spite of marginal progress. Irrespective of the recent innovative growth and development by woman and minorities in all aspects of industry, their representation in cybersecurity continues to remain dormant. Amid this remarkable growth and contribution, what is next? The first school of thought asserts that the unbalanced culture of women and minorities in cybersecurity is due to their incompetence, inability to advance in the profession, discrimination, and the feeling of inadequacy or simply male chauvinism. The second school of thought, the one I subscribe to, focuses on a more progressive and liberal view of women and minorities who have challenged the myopic concept of gender and racial inferiority. The continuing progress and groundbreaking shift in the millennial population evidences most women and minorities under the ages of 30-35 completing their undergraduate and graduate degrees in computer science and information security on the scheduled dates and time with males and other majority groups. Chabrow (2011), in his studies on women and minority scarcity in information technology (IT), cautions that the world community must continue to embrace the paradigm change of the millennial populace as a benchmark to eradicate gender penchant and men chauvinistic approach on unbalanced culture of women and minorities in the cybersecurity profession. Recognizing and supporting the millennial population's academic ambition and accepting them as active partners in cybersecurity professional is the way forward as a well-thought out measure to bridge the gender gap in the profession.

## Disproportionate Culture in Cybersecurity Operation

Shelving or ignoring women and minorities in cybersecurity operation is tantamount to the denial of equal opportunity to protect and defend the global community in the day-to-day battle against perpetrators of cyber-threat and cyber-attack. Per Benison (2009), Shumba (2013) and Brotherton & Berlin (2017), the remedy to decrease the disproportionate ethos of male dominant slant and enforcement of comprehensive mitigation plan of action must include collaboration and principled agreement between men, women and minorities, urging them to step out of insulated showground and be ready to defend and protect vulnerable citizens against imminent cyber-threats and cyber-attacks. The envisioned cybersecurity professional alliance must be structured to overcome human identity and accept the fact that cyber-threats and cyber-attacks are active and imminent living forces on the threshold of launching wide-ranging assault on men, women, minorities and organizations (Elan, 2012; Dallaway, 2013; and Weiss, 2016). Notably, the cyber world stands in need of collective strength against the current disproportionate slant of male, women and minorities to establish effective cyber-defensive and protective security mechanism to protect private and public organizations and innocent citizens. Women and minorities are engrained with an inexhaustible repository of untapped expertise that will inevitably prepare current and future cyber-experts in the battle against invisible every day and any moment perpetrators of cyber-attacks. As Weiss (2016) concludes in his studies, the biggest problem women and other minorities face in the workplace is the unequal treatment of women and minorities as a result of a narrow-minded discrimination grounded on the gender penchant for male chauvinism, and this unfortunate work relationship is detrimental to the global plan of action against the battle of cyber-threats and cyber-attacks.

I must admit that the response to "what is next?" is a sustainable collaboration and principled agreement between men, women and minorities to battle heartless perpetrators of cyber-attacks. Again, "what is next" must involve the eradication of men's narrow-mindedness, which has deprived capable women the opportunity to contribute to the defense against cyber-attacks. A plethora of women and other minorities have been trailblazers in cybersecurity operations and have accumulated untapped intellectual capability and the willingness to contribute to the stability of global economy and security. Today is the right time for the world of academics to tap into and use this knowledge for the protection of cyber development and safety.

## Women and Minority Intellectual Talent

Despite gender stereotyping and cultural beliefs about the intellectual and scientific inferiority of women and minorities, women and minorities continue to aspire as unwavering contributors in the battle against global security. As Esin (2019) noted, the 21st century women and minorities are ascending and matching the success ladders of their men counterparts. Unfortunately, women and minorities' contributions to cybersecurity profession are sidelined for no ostensible reason, except for the fact that the traditional and religious notion that tended to dictate gender relationships was that men were often projected as assertive, self-assured and formidable in the society. The women have been often been relegated to the home, childbearing and childcaring and cooking. However, and undeniably, women and minorities have also been the leading contributors in battle to defend and protect the global community:

* In 1940, Elizabeth Smith Friedman, (minority & woman) helped to invent the science of cryptography for the United States Federal Bureau of Investigation (FBI). Her techniques broke international spy rings decoded three Nazi Enigma machines and contributed to the early work of the forerunner to the Central Intelligence Agency (CIA). Right after the war, her elite code-breaking unit was shut down and various men took credit for her work (Poster, 2012; Browne, 2015; & Shumba 2013).

* In the 1950s, an African American female, Katherine Johnson, (minority & woman), a mathematician at NASA calculated the aeronautical trajectories to put Man on the Moon. The proportion of minority and women in computer science

grew until the mid-1980s. Again, right after the discovery, the dawn of personal computing evolved swiftly (Poster, 2012; Browne, 2015; & Shumba 2013).

* In 2009, Melissa Hathaway, (minority & woman) served as President Obama's first acting senior director on cyberspace for the National Security Council (NSC) (Poster, 2012; Browne, 2015; & Shumba, 2013).
* In 2004-2010, Letitia Long, (minority & woman) was the first woman director of the National Geospatial-Intelligence Agency which supplied the satellite, geographical and social-media data that enabled the capture of Osama bin Laden (Poster, 2012; Browne, 2015; & Shumba 2013).
* In 2013-2016, Dr. Jane LeClair (minority & woman) served as the Chief Operating Officer, providing outstanding leadership for the National Cybersecurity Institute dedicated to increasing knowledge and expertise in the cybersecurity discipline (Esin, 2018; LeClair & Keeley, 2015).
* From 2016 to present, Dr. Jane LeClair (minority & woman) established Washington Center for Cybersecurity Research and Development (WCCRD), an organization dedicated to the advancement of skills, knowledge and competency of minority women and men in cybersecurity education. She organized and convened conferences and training across the globe (LeClair & Pheils, 2016; & Esin, 2018).
* On January 19, 2019, thousands of women and minorities across fifty states of the continental United States were committed, dedicated and willing to strengthen their individual talents and protection of vulnerable citizens against cyber-attacks and cyber-crimes (Esin, 2019: Page. 6-7).

## Mitigation

Women and minorities' talents are often diluted, prohibited and dominated by male-dominating and Caucasian's majority approach often given limited or no line of authority. The egotistic and male narrow-mindedness often modulates minority and women's ability to become active operators in cyber-security that demands diverse skills, talents and intellectual contributions to battle perpetrators of cyber-attacks on vulnerable innocent citizens (Shumba, 2013; Benison, 2009; Ngwang 2018, Esin, 2019). Cybersecurity operations amplify the ethos of protecting and defending world organizations against cyber-threat; and echelons of battling cyber-attacks and cyber-threats is an all-embracing responsibility requiring participation and contribution of men, women and citizens of the global community. Today, cybersecurity unemployment rate has dropped to zero-percent; however, the global benchmark relative to talented cybersecurity professionals is not enough to curb the growing epidemic of cybercrime and cyber-attack and to counteract spiteful attacks against vulnerable innocent communities (Shumba, 2013; Benison, 2009).

There are millions of job opportunities ahead of the current and future generation; hence, the present-day parochial approach must be eliminated since no single entity has adequate resources to battle the global cyber-threats.  Per LeClair & Pheils (2016) and Shumba (2013), comprehensive outreach is key to eradicating existing cyber-attacks and this strategy must include and increase the low statistics of women and minorities entering the cybersecurity workforce. Private and public organizations and high education enterprises must be willing to step forward with significant plans of action to attract and retain women and minorities; otherwise the unbalanced culture of women and minorities in cybersecurity will continue inevitably to lead to the explosion of the impairment of global efforts to battle cyber-threats. Over a quarter-million positions in cybersecurity domain continue to remain unfilled in most nations and there is a projected shortfall of 1.5 million cybersecurity professionals in the United Sates by 2020 (Esin, 2018; Hu, 2014; and Elan, 2012). Men cannot only fill these positions. There are minorities and women willing and eager to fill these positions, but the intransigence of males and majority chauvinism stand in the way of positive engagement of these disadvantaged groups.

## Conclusion

Globally, there are not enough cybersecurity professionals and cyber operation is experiencing a growing shortage of skilled personnel. Men chauvinism and discrimination contribute largely to unbalanced culture of women and minority in cybersecurity domain.  Men often hold high-level directorship and managerial positions, whereas, women and minorities routinely occupy entry-level and nonmanagerial positions. It will take collective societal efforts to eradicate the looming inequalities and to dismantle the baggage of gender stereotyping that result in suppressing talented women and minorities from contributing to global security operations.

## References

Benison, L. (2009) “*Are men or women better at it” From* http://www.computerweekly.com/*News/2240089131/Are-men-or-women-better-at-it?*

Chabrow, E. (2011). Women, m*inorities scarce in IT Security Field*.” from http://www.bankinfosecurity.com/women-minorities-scarce-in-security-field-a-4143

Dallaway, E. (2013). *Let’s hear it for the ladies: Women in information security. From* http://www.infosecurity-magazine.com/magazine-features/lets-hear-it-for-the-ladies-women/

Elan, S. (2012). *Study: Women encounter inequality in science & technology fields. Retrieved from* --https://www.elsevier.com/connect/study-women-encounter-inequality-in-science-and-technology-fields

Esin, J. O. (2018). “Eliminating Gender Disparity in Cybersecurity Professions Through Education (WCCRD) **https://www.washingtoncybercenter.com/publications-projects**

Esin, J. O. (2019). A call for concern: The unbalanced representation of minorities’ and women in Cybersecurity Profession. From https://www.washingtoncybercenter.com/publications-projects

Hu, E. (2014) “Facebook’s Diversity Numbers Are Out, And They’re What You Expect,” http://www.npr.org/blogs/alltechconsidered/2014/06/26/325798198/Facebooks-diversity-numbers-are-out-and-they’re-what-you-expect.

Brotherston, L. & Berlin, Amanda (2017). Defensive security handbook-best Practice for securing infrastructure. Sebastopol: CA

LeClair, J. & Pheils, D. (2016). *Women in cybersecurity*. Albany, New York: Excelsior College Press.

Ngwang, E. N. (2018) The challenges of practical ethics and leadership in the age of cyber education: A crisis in management**.** *Journal of Educational Research and Technology (JERT)* 7 (7)

Poster, W. R. (2012). “Global technology diffusion and gender disparity: Social impacts of ICT.

Shumba, R. et al. (2013) “Cybersecurity, Women and Minority.” Proc, ITiCSE-WGR.

Tsai, P. (2016). “*Cybersecurity skills gap? Most organizations lack IT security experts*.” from https://community.spiceworks.com/topic/1618495-cybersecurity-skills-gap most-organizations-lack-it-security-experts

Weiss, S. (2016). “*The Biggest Problem Women Face in The Workplace Isn’t What You Might Expect.”* from http://www.bustle.com/articles/177461-the-biggest-problem-women-face-in-the-workplace-isnt-what-you-might-expect

## About the Author

### Joseph O. Esin, PhD

Dr. Joseph O. Esin is Professor of Computer Information Systems at Jarvis Christian College, Adjunct Professor of Cybersecurity-Defensive Security at Thomas Edison State University, and Visiting Professor of Research University of Calabar, Nigeria. He is also the former dean and deputy provost at Paul Quinn College.

# A Multiple Intelligence Soft Skills Guide for Leaders in a Multigenerational Workplace

Dr. Grace Miranda
Argosy University, Graduate School of Business and Management

Dr. Pamela Allen
Thomas Edison State University

## Abstract

In (2015) a qualitative research study explored the styles of leadership and diverse competencies that would enable leaders to lead multigenerational organizations (Miranda, 2015). However, significant results from this study continued to reveal valuable insights that are important for leaders who need additional levels of competency in a multigenerational workplace. The willingness to engage in intentional learning is required for seeking knowledge, awareness and skills that includes multiple types of intelligence consisting of emotional intelligence, ethical intelligence, social intelligence and spiritual intelligence. However, acknowledgement of artificial intelligence and combinations of artificial intelligence and robotics are essential considering the connection of these types of intelligence to current job-related skills in multiple industries. Development of new marketable skill sets will allow future leaders and workers the best opportunities to manage multigenerational competition. Developing soft skills such as leadership, communication, and teamwork will also provide additional tools for building organizational citizenship behaviors. This article is a multiple intelligence soft skills guide for leaders who want to be successful in a multigenerational workplace.

*Keywords: leadership, multiple generations, multiple intelligence, emotional intelligence, ethical intelligence, spiritual intelligence, social intelligence, artificial intelligence, soft skills, robotics*

Significant challenges for leaders in the new millennium involves a multigenerational workforce consisting of Traditionalists, Baby Boomers, Generation X, and Generation Y. Leaders in the modern multigenerational workforce continues to reveal struggles to understand the differences between multiple generations (Kirkpatrick, Martin, & Warneke, 2008) how to demonstrate the most effective leadership, and encourage communication and teamwork as valuable soft skills. However, additional recommendations from a qualitative study focusing on leading a multigenerational organization (Miranda and Allen, 2017) suggests that leaders engage in intentional learning about multiple types of intelligence while also demonstrating multiple soft skills for diverse work environments. The qualitative research study included observations from participants in focus groups. The first focus group included leaders of multigenerational groups employed within the United States. A second focus group included individual workers who were representatives of one of the four generations currently in the United States workforce that consists of Traditionalists, Baby Boomers, Generation X and Generation Y. A significant recommendation from the focus groups suggested that multiple intelligence and soft skills were necessary for leaders of a multigenerational workforce (Miranda and Allen, 2017). However, additional trends in the global workforce suggests more than one type of intelligence in addition to demonstrations of soft skills that involve leadership, communication and teamwork are also necessary (Carnevale and Smith, 2013). The purpose of this article is to provide what would be considered a practical and useful guide that expands the types of multiple intelligences, mentioned by participants in the research study (Miranda and Allen 2017) and combine them with other soft skills required for more effective leadership in a multigenerational workforce.

## Emotional Intelligence

Observations from the participants in the qualitative study indicated that emotional intelligence was an important ability to demonstrate to be a more effective leader in a multigenerational workforce. Baack (2017) describes emotional intelligence as the ability of an individual to detect and manage emotional cues and information. A more detailed description of emotional intelligence is separated into five dimensions.

1. Self-Awareness
2. Self-Management
3. Self-Motivation or Self-Persistence
4. Empathy
5. Social Skills

"Demonstrating emotional intelligence is an acquired skill that allows individuals to manage themselves and their work-related relationships. Individual understanding of the power of emotions and mastering the ability to manage and express emotions could enhance an organization's effectiveness significantly" (Miranda and Allen, 2017). However, during discussions in the focus groups participants also included the need for social intelligence for individuals leading a multigenerational workforce.

## Social Intelligence

Dewey (1909) and Lull (1911) as cited in Kihlsrom and Cantor (2011) were the first individuals to use the term “social intelligence. Initial efforts to explore how to think and behave during human situations, is a description of social intelligence developed in 1920 by E. L. Thorndike. A social intelligence profile was developed by Albrecht (2009) who placed five basic skills in a category to describe social intelligence including a. situational awareness b. presence c. authenticity d. clarity and e. empathy. However, in 2006 Goleman continued the evolution of social intelligence by adding “social skills” so that the individual demonstrates:

1. Appropriate self-expression
2. Insightful observations
3. Understanding during social interactions

However, trends in the work environment suggests that additional types of intelligence should be part of the leadership skillset to address significant issues occurring in the present and included in predictions for the future. Ethically Intelligent Leaders, Spiritual Intelligence, and Artificial Intelligence.

## Ethical Intelligence

Ethically Intelligent Leaders An insightful and thought-provoking description of ethical intelligence was developed by John T. Opincar in his book “Ethical Intelligence: The Foundation of Leadership.” In the final chapter the author describes the ethically intelligent leader by suggesting, “For leaders, every leader/follower relationship is a garden. Into that garden we sow seeds of hope, recognition and expectation. We fertilize those seeds with teaching and direction.
We water with encouragement and understanding. We cultivate with a vision of our destination. We weed with assessment and feedback. We prune by allowing mistakes. Through it all, we set clear expectations for a bountiful harvest. Those who master this new art of relationship gardening will become the great ethically intelligent leaders who change the world.” (Opincar, 2016, p. 332). Leaders of a multigenerational workforce would benefit from demonstrating this type of ethical intelligence that would be an active application of ethical thoughts, attitudes, and behaviors. But, also consider that spiritual intelligence would be a valuable addition to complement emotional intelligence, social intelligence and ethical intelligence.

## Spiritual Intelligence

Developing the ability to identify and reconnect with some meaningful and authentic purpose in an organizational environment are important aspects of spiritual intelligence (Scharmer, 2009). Wigglesworth (2012) distinguishes spiritual intelligence from spirituality or religion and frames it as a set of skills. This type of intelligence is associated with “the ability to maintain complete peace while demonstrating wisdom and compassion regardless of the circumstances (p.4). Application of spiritual intelligence to different generations in the workforce would reveal valuable information about what is meaningful; what defines authenticity and purpose; and what goals are important to achieve according to unique generational perspectives. Kaur and Kaur (2015) expand on the demonstration of spiritual intelligence that includes high levels of growth associated with the ability to adapt, and problem solve within the following domains a. cognitive b. moral c. emotional and interpersonal. However, another level of growth for leaders of multiple generations in the workforce involves acknowledgement of artificial intelligence and robotics. The current and future workforce will involve customer interactions that are managed by a non-human agent and diverse self-service technologies.

## Artificial Intelligence and Robotics

Why AI? Because leaders in a multigenerational workforce who seek knowledge, abilities and skills including a combination of artificial intelligence and robotics will replace those who choose not to prepare diverse workers for the present and future. Hyacinth (2017) describes artificial intelligence as a type of computer science dedicated to the creation of machines or programs capable of demonstrating multiple types of intelligence without programmed instructions. Intelligent machines would have the ability to think, learn and imitate human reactions. Software and hardware technologies would be part of an AI system with the ability to use multiple intelligence to communicate, reason and predict at a significantly faster speed than humans.

At this point there must be some clarification that would answer the question if robotics and artificial intelligence are related? Artificial intelligence and robotics are different fields of study. A simple example in the manufacturing industry would be programming a robot in a factory to perform repetitive tasks with real objects or things. However, artificial intelligence involves creating algorithms embedded in machines that allow making decisions, change, and improvement without the direction or control from human beings. Multiple industries are currently experiencing or will experience the impact of artificial intelligence and robotics.

Table 1 summarizes information obtained from The Pew Research Center regarding jobs, services and operations where artificial intelligence and robotics will have a significant impact by 2025. However, significant changes are currently evident in multiple industries.

| Industry | Job/Service/Operation<br>and<br>Impact of Artificial Intelligence and Robotics |
|---|---|
| Domestic | Cleaners, Homecare, Nanny, Companion |
| Commercial | Packing, Drawing, Printing, Media, Pharmacy, Retail, Hospitality |
| Transportation | Cab, Truck Drivers, Waste Removal Truck Drivers |

| | |
|---|---|
| Medical | Hospital, Surgery, Diagnostics, Disease Scans, Cancer Scans |
| Industrial | Repetitive Tasks in Factories and Farms, Hazardous Waste Management, Nuclear Disaster Recovery and Containment |
| Sea | Salvage and Recovery Operations |
| Law and Enforcement | Police and Traffic Officers |
| Military | Soldiers, Drones, Tank Drivers, Disarming Bombs |
| Space | Construction, Digging, Maintenance on Space Stations, Space Exploration |

Table 1

Leaders of individuals in a multigenerational workforce would benefit from knowledge, ability and skills that includes multiple intelligences that apply to jobs, services and operations that are essential parts of the diverse industries mentioned in the research. But, there must also be consideration of skills-oriented learning as a global work initiative.

## Skills Oriented Learning

The Organization for Economic Cooperation and Development (OECD) survey of adult skills emphasizes the interdependence of humans and societies (The Organization for Economic Cooperation and Development, 2017). An important observation in the survey suggests a particular set of skills for global workers to continue learning throughout their lifetime (The Organization for Economic Cooperation and Development, 2017). In the section of the survey for maintaining work-related skills the following recommendations are significant “In high-technology sectors, workers need to update their competencies and keep pace with rapidly changing techniques. Workers in low-technology sectors and those performing low-skilled tasks must learn to be adaptable, since they are at higher risk of losing their job as routine tasks are increasingly performed by machines, and since companies may relocate to countries with lower labor costs.” (OECD, 2017).

## Soft Skills in a Multigenerational Workforce

The results of this research also suggested that employees of multi-generational organizations/groups still require that they be respected, treated fairly, and they have desires to work in an atmosphere that satisfies their needs.

## Results

The participants of each group are representatives of varying work industries and generations in the United States. Focus Group One consisted of six participants (leaders) representing all four generations. The following is a generational description of each participant: One Traditionalist (born 1912-1945), two Baby Boomers (born 1946-1964), two Xers (born 1965-1979) and one Y (born 1980-1995). The second Focus Group consisted of six participants who also represented all of the four generations. Generational demographics for Focus Group Two are as follows: One Traditionalist (born 1912-1945), two Baby Boomers (born 1946-1964), two Xers (born 1965-1979) and one Y (born 1980- 1996). The demographic description of the participants was derived from the American Management Association [AMA] (2015). The focus groups were held a week apart. Upon completion of the first focus group, transcription of the audiotaped discussion data analysis was initiated. A pattern was uncovered indicating some of the responses from Focus Group Two were identical or similar to words and phrases used by Focus Group One (leaders).

Results from the data analyses revealed that the self-developed questions designed for the focus group discussion and research objectives elicited the responses needed to address the research question. The data from both focus groups detected a set of themes and ideas that divulged fresh insights of the crucial dynamics that addresses some of the challenges faced by leaders of multigenerational organizations/groups in the United States.

The results indicated that utilization of the following three leadership styles would be beneficial to all generations in the current workplace due to the affirmative effect of leaders towards employees, and organizations. The Authentic, Ethical, and Servant Leadership styles, when utilized in leading the four generations currently working in the U.S. workforce, would be effective. The participants' responses indicated that the practices of emotional and social intelligence, as well as empathy, were essential in leading the wide variety of employees present in modern work environments.

## Conclusions and Recommendations

Legault's (2002) findings indicated that each of the four generations included in Summary, her study had commonalities, such as desires to be respected, treated fairly, and to work in an atmosphere that fulfilled their needs. Legault also recommended that future research should be conducted to provide organizational leaders with expertise in decision-making skills and strategies to address the differences and similarities of an age diverse workforce. To follow and build on Legault's study, an inductive exploratory strategy was utilized, in order to estimate the most effective method to produce data with a high degree of transparency and reliability, which provided awareness of limitations and biases (Reiter, 2013).

The findings confirmed, as asserted by Legault's (2002) study, that the four generations have differences and similarities more than a decade later. The results of this research also suggested that employees of multi-generational organizations/groups still require that they be respected, treated fairly, and they have desires to work in an atmosphere that satisfies their needs.

In addition, Legault emphasized the importance of meeting the individual needs of generational cohorts to effectively lead multiple generations. The examination of leadership styles and relational skills in this study confirms that a change of leadership style and the enhancement of relational skills could meet the needs of each generation. The findings from the data analysis, along with the literature, indicated that leaders are currently encountering challenges in leading multiple generations.

## Relevant Themes

The findings from the data analyses were used to address the research question along with literature that confirms that the findings are valid and reliable. The following themes derived from the focus group discussions addresses the research question: 1. Emotional and Social Intelligence 2. Motivation 3. Communication 4. Work/Life Balance 5. Time 6. Hierarchy 7. Respect and Hard Work 8. Support of Generational Differences. These themes represent some of the challenges leaders face in leading and working with multiple generations, according to the focus group comprised of leaders.

The findings of the research study also affirm the leadership styles (Authentic, Ethical and Servant Leadership) to be valuable in leading a multigenerational organization/group coupled with the application of the relational skills of emotional and social intelligence and the components of SMILE. According to Walumba, Wang, Wang, Schaubroeck, and Avolio (2010), Authentic Leadership behaviors could improve employee engagement and organizational productivity based on their acceptance of the opinion of others, openness, sharing information, generously, regarding decision-making processes, as well as demonstrating transparency professionally and personally. Ethical leaders focus on making fair decisions and on listening, in addition to utilizing and encouraging collaborative communication (Brown, Trevino, & Harrison, 2005). A servant leaders' goal is to create opportunities for employee empowerment and success. Washington, Sutton, and Field (2006) reported that servant leaders possess the unique qualities of empathy, integrity, and competence, which are principles of efficient leaders. Each of these leadership styles exhibits competency in empathy and emotional and social intelligence, making all of them capable of meeting the needs of multiple generations based on the findings of the research study.

Also confirming the study's findings is Daft's (2008) description of emotional intelligence as "a person's abilities to perceive, identify, understand, and successfully manage emotions in self and others" (p.143). The five components of emotional intelligence, which are self-awareness, self-regulations, motivation, empathy, and social skill (Goleman, 2004), were referenced by the study's participants as being important abilities for an effective leader to demonstrate. In addition, both Dearborn (2002) and Goleman (2004) agreed that emotional intelligence could be learned and would require practice over a period of time before a leader is considered proficient. The leaders in focus group one also stated this perception.

Marques (2011) introduced the SMILE concept, which is an acronym for the concepts of spirituality, meaning, interbeing, leadership, and empathy, which are embraced as a means to build and support human interactions. The SMILE concept was not introduced to the focus group; however, it confirms the findings of this study and collaborates with the five components of emotional intelligence and the five basic skill groupings of social intelligence. The following describes how the SMILE theory confirmed the findings of this study: the concept of spirituality refers to a worker who maintains goodwill by supporting and respecting other workers. Meaning is the concept that allows leaders to value the work/life balance desired by their employees. Interbeing is the change needed to ensure that everyone is perceived as having value to the organization/group and should receive this type of response. Leadership must value employees and demonstrate so by listening, engaging, and appreciating them. Empathy is the connection needed to understand the emotions of employees during difficult situations and problems.

## Recommendations

The recommendations consist of implications for practice with multiple strategies from a variety of sources. They also present implications for future research with lessons learned.

### Implications for Practice

Based on the review of the literature and the responses from the two focus groups, the implications for leaders are to shift their perspectives and embrace change is clear. Recommendations for change includes taking the time required to understand that each generational cohort has expectations that differ (Hammill, 2005). Therefore, it is important for leaders to reflect a leadership style that accommodates the demands of each generation, as their needs are different (Salahuddin, 2010; Crampton & Hodge, 2007; DiCecco, 2006, & Hammill, 2005).

### Strategies for Leadership Competency

One strategy for the development of competent leadership could be to utilize training programs focused on the development of emotional intelligence. Leaders could attend this type of program with their employees, modeling openness to acknowledge and address their employees, which would be beneficial to both leaders and employees. The benefit to the leader is the ability to foster a work environment of collaboration. The benefit to the employees is the ability to recognize and respect their own emotions and the emotions of others in their work environment.

Another strategy for the development of self-awareness, to achieve maximum performance, is for everyone in the organization, both leaders and employees, to take an emotional intelligence assessment. This type of measurement could highlight strengths and identify areas of improvement for each individual. The leader could follow-up with the employees individually to map out a plan to strengthen areas of improvement. This strategy could reduce the tendency to stereotype each generation within the organization/group culture. Bruce and Montanez (2012) stated, "Working in a multi-generational workplace is not a task for the weary or weak -- but the strong and determined" (p. 29). Bruce and Montanez describe the following strategies that, with consistent implementation, can be learned and mastered: a. “utilization of multiple communication channels ( everyone approaches communication differently) b. foster a flexible environment focused on productivity (again everyone has preferences on what environmental factor influence them to generate excellent performance) c. encourage open communication (leaders create a safe atmosphere where everyone learns to accept the communication styles of others including maintaining respect and professionalism); set goals and expectations (with processes in place affords leaders an opportunity to be flexible across the board)” (p. 29-30).

Society for Human Resource Management (SHRM, 2004) suggested strategies for individual generations. For the Traditionalist, leaders should illustrate compassion and comprehension to secure their employees’ confidence. They should establish optimistic working relationships with the Traditionalist. Acquiring the Traditionalist’s trust and expressing respect for his/her experience without being threatened by it could accomplish this. For the Baby Boomers, leaders should display appreciation for their vigor and hard work, respect for their accomplishments, employ a mutual leadership style, and present opportunities for them to serve as a coach as part of any change processes. In addition, leaders should allow this generation to participate in the change initiatives. Regarding Generation X, leaders should be truthful, provide mentoring programs, clarify boundaries, and respect their need for work/life balance. Finally, for Generation Y, leaders should utilize technology for communication with them, such as emails and text messages. Also, leaders should reinforce the value this generation adds to the organization/group and provide public praise. The strategies from Bruce and Montanez (2012) and SHRM (2004), along with the findings from both focus groups, are approaches that could be beneficial for leaders of multi-generations to implement in order to meet the goals of the majority of their employees.

## Future Research

If leaders adopted the implication for practice and implemented some of the strategies provided in the results from this research study, the dynamics of the relationship between leaders and employees of multiple generational organizations/groups would eradicate many of the significant challenges. Additionally, if leaders of multi-generational organizations/groups employ the recommendations and strategies, leaders may discover, by utilizing both the commonalities and differences between the generational cohorts, they will have the capacity to build a cohesive and successful work environment.

## References

Adecco. (2009). Managing today’s multigenerational workforce. Retrieved from http://www.adeccousa.com

Albrecht, K. (2009). Social Intelligence. The new science of success. Personal Excellence, 10, (12), 5.

Ahlrichs, N.S. (2007). Managing the generations differently to improve performance and profitability. Employment Relations Today, 21-31. doi:10.1002/ert.20138

Aker, J. M. (2009). Managing a multigenerational workforce. Buildings, 103(1) 46-48. Albrecht. K. (2009). Social intelligence: The new science of success. Personal Excellence,10 (12), 5.

American Management Association (2015). Leading the four generations at work. Retrieved from http://www.amanet.org/trauning/articles/Leading-the-Four-Generations-at-Work.aspx

Brinckerhoff, P. C. (2007). Generations: The challenge of lifetime for your nonprofit. Saint Paul, MN: Fieldstone Alliance.

Brown, M. E., Trevino, L. K., & Harrison, D. A., (2005). Ethical leadership: A social learning perspective for construct development and testing. Organizational Behavior and Human Decisions Processes, 97: 117-134.

Bruce, A. & Montanez, S.M., (2012). Leaders start to finish: A road map for developing to performers (2nd. Ed.). ASTD Press, Baltimore, MD..

Cantor, N., & Kihlstrom, J. F. (1987). Personality and social intelligence. Pearson College Division.

Carnevale, A. P., & Smith, N. (2013). Workplace basics: The skills employees need employers want. Human Resource Development International, 16(5), 491-501. http://dx.doi.org/10.1080/13678868.2013.821267

Conger, J. A., & Pearce, C. L. (2003). A landscape of opportunities: Future research on shared leadership. In C.L. Pearce & J.A. Conger (Eds.), Shared leadership: Reframing the hows and whys of leadership (pp. 285-303). Thousand Oaks, CA: Sage.

Crampton, S. M. & Hodge, J. W. (2007). Generations in the workplace: Understanding Age diversity. The Business Review, Cambridge, 9(1), 16-22.

Crumpacker, M. & Crumpacker, J. (2007). Succession planning and generational stereotypes: Should HR consider age-based values and attitudes a relevant factor or a passing fad? Public Personnel Management, 36(4), 349-369.

Daft, R. L. (2008). The leadership experience. (4th ed., pp. 313 & 396). Mason, OH: Thomson South-Western.

Dearborn, K. (2002). Studies in emotional intelligence redefine our approach to leadership development. Public Management; ABI/INFORM ; 31(4); pg. 523.

DiCecco, V. (2006). Hey…What’s the matter with kids today? Managing today’s- cross generational workforce. Retrieved from http://www.sgia.org/feature_articles/kids_today_dicecco.htm

Dorset, G. J. (2008). The new American workplace: Generational diversity from four participating cohorts offering challenges, obstacles, and opportunities for success (Doctoral Dissertation). Retrieved from ProQuest Dissertations and Theses. (UMI No. 89279729)

Fraone, J. S., Hartmann, D., & McNally, K. (2009). The multi-generational workforce: Management implications and strategies for collaboration. Boston College Center for Work & Family Executive Briefing Series. Retrieved fromhttp://www.bc.edu/centers/cwf/research/publications/metaelements/pdf/MultiGen_EBS.pdf

Goleman, D. (2004). What makes a leader? Harvard Business Review. Retrieved from: http://hbr.org/2004/01/what- makes-a-leader/ar/1

Goleman, D. (2006), Social Intelligence: The New Science of Social Relationships, New York, Bantam Books.

Guest, G., Bunce, A. & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. Field Methods, 18(1), 59-82.

Hammill, G. (2005). Mixing and managing four generations of employees. Retrieved from http://www.fdu.edu/newspub/magazine/05ws/generations.htm

Jeter, M. (2008). Managing the multigenerational workforce: Meeting the unique needs of the Traditionalists, Generation Xers, and Millennials. Retrieved from http://www.lakeshorestaffing.com/downloads/articles/251.pdf

Kai-Wen, C. (2014). A Study on applying focus group interview on education. Reading Improvement, 51(4), 381-384.

Kaur, H. & Kaur, P. B. (2015). Relationship between spiritual intelligence and core life skills Of pre-service teachers. Contemporary Research in India, 5(3),129-135.

Keane, S., Lincoln, M., & Smith, T. (2012). Retention of allied health professionals in rural New South Wales: A thematic analysis of focus group discussions. BMC Health Services Research, 12, 175. doi:http://dx.doi.org/10.1186/1472-6963-12-175

Khilsrom, J. F. & Cantor, N. Social Intelligence. In The Cambridge Handbook of Intelligence (1st ed., p. 564). New York, NY: Cambridge University Press.

Kirkpatrick, K., Martin, S., & Warneke, S. (2008). Strategies for the intergenerational workplace. Retrieved from http://www.gensler.com/uploads/documents/IntergenerationalWorkplace_07_17_2008. pdf

Kouzes, J.M., & Posner, B.Z. (2007). The leadership challenge (4th ed.). San Francisco, CA: John Wiley & Sons.

Kress, V. E., & Shoffner, M. F. (2007). Focus groups: A practical and applied research approach for counselors. Journal Of Counseling & Development, 85(2), 189-195

Krueger, R.A, & Casey, M.A., (2015). Focus groups: A practical guide for applied research (5th ed.). Thousand Oaks, CA: Sage.

Leedy, P.D. & Ormond, J.E. (2005). Practical research: Planning and design. (8th ed.). Upper Saddle River, NJ: Merrill Prentice Hall.

Legault, M. (2002). Bringing people together: A study of generational diversity and organizational culture (Doctoral dissertation). ProQuest Dissertations and Theses database. (UMI No. 305485706)

Lowe, D., Levitt, K. J., & Wilson, T. (2008). Solutions for retaining generation Y employees in the workplace. Business Renaissance Quarterly, 3(3), 43-57.

Magnuson, D. S., & Alexander, L. S. (2008). Work with me: A new lens on leading the multigenerational workforce. Minneapolis, MN: Paradigm Publishers.

Marques, J. (2011). Five principles that will determine the new mainstream: Spirituality, meaning, inter-being, leadership and empathy: SMILE. Human Resource Management International Digest, 19(4), 39-42.

Miranda, G. (2015). Leading A Multi-Generational Organization: What is Needed? (Unpublished Doctoral Dissertation). Argosy University, Florida.

Miranda, G. & Allen, P. (2017). Strategies for leading a multi-generational organization. i-manager's Journal on Management, 12(2), 14-25.

Moore, S. K., Guarino, H., Acosta, M. C., Aronson, I. D., Marsch, L. A., Rosenblum, A., & ... Turk, D. C. (2013). Patients as collaborators: Using focus groups and feedback sessions to develop an interactive, web-based self-management intervention for chronic pain. Pain Medicine, 14(11), 1730-1740. doi:10.1111/pme.12200

Murphy, S. (2007). Leading a multigenerational workforce. AARP, Clare Raines Associates.

Nicholas, A. J. (2008). Millennial interest in teleworking. (Doctoral dissertation). ProQuest Dissertations and Theses. (UMI No. 304703062).

Opincar, J. T. (2016). Ethical intelligence: The foundation of leadership (1st ed,). Houston, TX: Cultural Fire Press.

Paris, M. J. (2008). Do generational differences really impact the workplace? Retrieved from http://ezinearticles.com/?Do-Generational-Differences-Really-Impact-the-Workplace?&id=1654858

Patton, M. Q. (2002). Qualitative evaluation and research methods (3rd ed.). Thousand Oaks, CA: Sage Publications.

Salahuddin, M. M. (2010). Generational differences impact on leadership style and organizational success. Journal of Diversity Management, 5(2), 1-6.

Scharmer, C. O. (2009). Theory U: Leading from the future as it emerges. San Francisco, CA: Berrett-Koehler.

Schneider, S. K. & George, W. M. (2011). Servant Leadership versus transformational leadership in voluntary service organization. Leadership & Organizational Development Journal, 32(2), 60-77. doi: 10.1108/01437731111099283

Singh, K. (2007). Qualitative social research methods. Thousand Oaks, CA: Sage publications.

Society for Human Resource Management, (2004). Leadership styles series part ii: Leadership styles. Society for Human Resource Management. Retrieved from http://multigen.shemindia.org/resources/articles/leadership-styles-series-part-iileadership-styles-generational-difference.

Stanley, A. (2003). Next generation leader: Five essentials for those who will shape the future. New York, NY: Multnomah Publishers, Inc.

Stevens, R. H. (2010). Managing human capital: How to use knowledge management to transfer knowledge in today's multigenerational workforce. International Business Research, 3(3), 77-80.

Thorndike, E.L. (1920). Intelligence and its users. Harper's Magazine. 140. 227-235.

Van Houdt, S., Sermeus, W., Vanhaecht, K., & De Lepeleire, J. (2014). Focus groups to explore healthcare professionals? experiences of care coordination: Towards a theoretical framework for the study of care coordination. BMC Family Practice, 15(1), 1-20. doi:10.1186/s12875-014-0177-6

Walumbwa, F. O., Wang, P., Wang, H., Schaubroeck, J., & Avolio, B. J. (2010). Psychological processes linking authentic leadership to follower behaviors. The Leadership Quarterly, 21, 901-914.

Washington, R. R., Sutton, C. D., & Field, H. S. (2006). Individual differences in servant leadership: The roles of values and personality. Leadership & Organizational Development, 27(8), 700-716. doi:10.1108/01437730610709309

Wendover, R. W. (2006). Generational shift: How emerging managers will alter the government finance leadership paradigm. Government Finance Review, 22(2), 90-92. Retrieved from http://www.allbusiness.com/

Wigglesworth, C. (2012). The 21 skills of spiritual intelligence. New York, NY: Select Books, Inc.

Wilson, L. (2009). Generations at work: The problems, power, and promise explored. American Water Works Association Journal, 101(5), 46-46.

## About the Authors

### Grace Miranda, EdD

Dr. Grace Miranda works with individuals and organizations, she builds leadership competency and confidence through coaching and consulting.  She has recently worked with the Armed Forces Servicers Corporation, Global University in Distance Education, and NeighborWorks America.

### Pamela Allen, PhD

Dr. Pamela Allen is a Faculty Mentor at Thomas Edison State University and CEO of a Woman-Owned Small Business. She continues to publish and present topics at national and international conferences including non-traditional approaches of managing diverse issues involving adult students, faculty and technology in higher education.  She contributed a chapter on the topic of leadership in the book *Diversity and Inclusion in the Global Workplace* in 2017 and another presentation occurred in Rome, Italy, in 2018, at the XIII International GUIDE Conference, “The Fourth Industrial Revolution in Higher Education-The age of Learning Management Systems.” She is a member of the Accreditation Council for Business Schools & Programs.

# I’m Faking The Causes and Implications of Imposter Syndrome for Women in the Field of Emergency Management and Homeland Security

Emily Kies
Elgin Community College

## Abstract

Many women who work in male dominated fields often question their abilities and qualifications. They sometimes feel that they do not deserve to occupy these positions. This is a condition known as Imposter Syndrome. This article defines this syndrome, identifies its causes, and provides insights on how to deal with it.

*Keywords: women, imposter syndrome*

“I’m faking it. It’s probably because I know the Chief. Great, one of three women in a room of 50, again.” I was suffering from Imposter Syndrome, but thankfully, I was not alone. It struck me how prevalent this condition was while reading an article written for Women’s Health Magazine. It was refreshing to finally put a name to a nagging feeling and hear other women share similar stories of their thoughts and feelings. After investing some time in researching this condition, the findings point to an increase in women entering career fields traditionally held by men. It would stand to reason that even a cursory review of this syndrome given to both men and women in traditionally male-dominated fields could alleviate some of the more negative symptoms of Imposter Syndrome.

What is imposter syndrome? Imposter Syndrome was initially coined during the 1970s. The first paper to use the term imposter phenomenon was published in Psychotherapy by Pauline Clance and Suzanne Imes in 1978. It is the basic belief that despite ones' achievements, accomplishments, credentials, and support of other professionals, they are not deserving of the position, compensation or other benefits that they currently receive and that they somehow achieved the degree of success due to luck or oversight on behalf of the individuals that have hired them into that position. Also, the individual feels that at any given time, the governing bodies will stumble upon some perceived evidence and “expose” them as the fraud that they believe they are. It’s very important to note that Imposter Syndrome is not a way to rename low self-esteem. A certain degree of self-esteem is required to set and achieve the goals that have resulted in the position that the individual currently holds. This continues to be a factor in the lives of women entering traditionally male-dominated fields, including Emergency Management, Homeland Security, and Cybersecurity.

For the most part, I have been lucky. As a woman in Emergency Management, I have not run into major disadvantages that come from being the minority. I have always gravitated to projects and opportunities that required a bit of ingenuity and creative solutions. I started as a volunteer and learned all I could about the field. It was a natural fit to complete my degree in Emergency Management and Homeland Security. It wasn't until I had been steadily working my way up the ladder of opportunities that I started to notice something peculiar. I was surrounded by mostly men. Let me emphasize that no one pointed out that I was the only woman in the room, yet the stage had been set. Like buying a new car and noticing how many of that model are on the road, I started to count the number of women in the room at various events. When attending conferences, it became apparent that the majority of the keynote speakers were men. I started to internalize a feeling of being the only one, and it quickly grew into something more. I would actively wonder if the recent opportunity that I had gotten was because I was a woman in a male-dominated field. Were they just trying to appease the diversity card?  When I share my title with the people, I often get raised eyebrows which I quickly explain away with comments like "it's not as cool as it sounds. No, I don't carry a gun." I had developed full-blown Imposter Syndrome. Freelance Software Engineer Katie Scheer writes:

> "When the new-job euphoria wore off, my thinly grasped gender pride took a paranoid turn. I wasn't surrounded by awesome teachers and peers who didn't make any deal of my gender, but instead by people surprised and curious to see me on the development side of the building, and this nagged at me. It made me self-conscious. When my comments or criticisms were dismissed, I started wondering if it was because I was a junior programmer, or because I was female. I had sort of taken on the little sister vibe. Maybe they'd settled for a sub-par hire just because I was a girl?" (Scheer, 2015)

The symptoms of Imposter Syndrome are in keeping with the name; they are an attempt to explain away current successes, an inability to internalize past or present accomplishments, and a fear of being "found out." In an effort to explain away current successes, sufferers of Imposter Syndrome will come up with a creative and lengthy list of all the reasons that they got where they are. Their thoughts may include internal dialogue such as "I got lucky, I was in the right place at the right time, it's because they like me/ think I'm pretty/ they felt sorry for me, if I can do it anyone can."

External dialogue may include comments similar to the following "A student in microbiology engineering quickly sets the record straight to those who are impressed by her field of study by explaining that it just 'sounds impressive because it has a long name'(Young, 2011, 20). This excuse rang especially true for me, as I routinely articulated the same sentiment when individuals were impressed by my Bachelor of Science in Emergency Management and Homeland Security. Other symptoms include the individual believing that they have somehow "fooled" the powers-that-be. This feeling appeared to be especially true if there was an inability to internally or externally explain away their success. In an imposter's mind, one success is unrelated and irrelevant to the next. "Rather than being cumulative, each accomplishment is its own sum game." (Young, 2011, 21).

The anxiety and fear caused by this syndrome can have severe negative impacts on the person's quality of life, in the belief that they are a fraud waiting to be found out. It also results in extremely qualified professionals second-guessing themselves for positions and opportunities, that in truth, they are perfectly able to hold, teach and would contribute greatly to the field. As an emerging profession, emergency management, homeland security, cybersecurity, and other areas cannot afford to have a growing percentage of their professionals sit back and fear to raise their hand or speak up. It's time to have a seat at the table and be the decision maker they are clearly qualified to be.

If a woman enters a field where she is already the minority and her very appearance conflicts with the status quo, this may set her up to feel as though the chips are stacked against her. She may feel the need  to work twice as hard to be valued half as much. E. Pittman, in Emergency Management Magazine, has echoed these sentiments, she states:

> "Marg Verbeek, an associate with Good Harbor Consulting and past president of the International Association of Emergency Managers, said that when she attended conferences 20 years ago that brought together as many as 500 participants, only a handful of women were present. And even today, when it comes to high-level roles, there are few women heading state offices" (2011,  20).

An important factor is the distinct differences in how men and women react to constructive criticism and how for some it can be internalized as a failure rather than as an opportunity for growth. Known as the self-regarding attribute bias, Dr. Sheila Widnall, MIT professor of aeronautics and astronautics & former secretary of the US Air Force, states -- "Treat a male student badly and he will think you're a jerk. Treat a female student badly and she will think you have finally discovered that she doesn't belong in engineering" (Young, 2011,48). This is a very important bias to be aware of, especially for males and females, where the blame for failure is placed and how corrective action can be made. The findings continue to support that women are a minority in these fields, and as such, the internal and external processes that they use to navigate their professional career path will be different than a male yet are just as valuable and require attention and care to flourish.

There are several ways to address and manage Imposter Syndrome, they begin with correcting the framework that some individual views their profession through. In Many Women Strong, the author suggests that:

> "A new female firefighter looks at the fire station as an environment dominated by male culture and a little like traveling to another country, where you have to get along in place very different from your own home. Being able to communicate with and understand others from different backgrounds in a bi-cultural atmosphere may be a positive way to accept the challenge as opposed to feeling a need to change who you are" (1999, 23).

Additional ways to address and alleviate the negative effects of Imposter Syndrome include developing working groups that encourage the discussion of this topic for women at all levels within professional sectors, as well as those women who have achieved great levels of success with sharing their stories. These stories, of both  success and failure, help pave the way for  women following in their path. Simple activities such as defining one's successes without additional justification are incredibly powerful. A simple list of accomplishments, degrees, promotions, awards, and letters of recommendation listed without additional justification is a way to start to adjust the mindset of someone with Imposter Syndrome.

Some of the most influential women in a variety of fields have suffered from some aspect of Imposter Syndrome. Take for example Piker's recall of Dr. Margaret Chan, the former director of the World Health Organization:

> "Her ability, conviction, and good judgment saved countless lives. But Dr. Chan discounted her native smarts – and the opportunity to promote herself – attributing it all to luck. Another public health expert physician, an acquaintance of mine, once told me that her expertise in tuberculosis is "a fluke." She travels the world to give lectures. She talks to the media and helps draft policy. Yet the diminutive, sharply dressed doctor has wondered aloud why people treat her with deference. "There are an awful lot of people out there who think I'm an expert. How do these people believe all this about me? I'm so much aware of all the things I don't know" (Piker, 2009, 183-184).

There is a place for the qualifiers; it's just changing the place that they hold in the mind of someone struggling to own their successes. Success and perceived qualifiers are not mutually exclusive. This is an important and significant change in mindset that can be extremely helpful. Luck, a winning personality, even one' professional image does play a role; re-framing the role that they play is needed. T For example, knowing the Chief of Police and that may have given me the initial opportunity to make a connection, but that's where the qualifier ended. These qualifiers can be found in most stories of success making them the rule, not the exception. Take for instance the story of a noted national security consultant for Northrop Grumman, Jeff "Skunk" Baxter. According to the Wall Street Journal, the Steely Dan guitarist received a subscription to an aviation magazine after mentioning his interest to a neighbor — who happened to be a former Pentagon engineer — which led him to wonder if existing military systems could be adapted to serve other purposes. Armed with time and interest, Baxter wrote a five-page paper suggesting that the military's ship-based Aegis anti-aircraft system could be converted into a missile-defense solution. He took the paper to Rep. Dana Rohrabacher, who in turn passed it on to Rep. Curt Weldon. Both were amazed, and Baxter was quickly drafted into service as a consultant. In addition to the U.S. Department of Defense, he's done work for the Pentagon's Missile Defense Agency, National Geospatial-Intelligence Agency and private defense innovators such as Northrop Grumman (Bonderun, D. May 24th, 2017).

Being able to identify thoughts that either were not accurate or incomplete went a long way in silencing my inner doubt. By changing the way I thought about my success and changing my internal dialog, changed the relationship I had with my accomplishments. This change in thought process, in turn, changed the way that I approached various opportunities. I spoke up. I understood that my success was a sum game, that each component was not an individual score. It was like sitting half-way up a very tall tower, and my previous thoughts created a fog, preventing me from clearly seeing the foundation I had built, leaving me to the belief that I had somehow faked my way to where I sat. By changing the way I thought of my previous experiences and successes, I cleared the fog and could see the foundation that led to my current position. As more women and underrepresented individuals enter fields such as Emergency Management, Homeland Security, Cybersecurity, the internal challenges they face must not be diminished by the external challenges of being the minority in a given situation. The benefit to the organization that pursues this kind of diversity is far-reaching and beneficially transformational in how the organization stays relevant and continues to deliver its mission. Women in a male-dominated field will process their business decisions through a lens that may be vastly different than that of their counterparts and these results can lead to  or more effective, results.

## References

Bonderud, D. (May 24th, 2017). From Music to Missile Defense: the Very Interesting Life of Jeff Baxter. Retrieved from: http://now.northropgrumman.com/.

Clance, P. R. and Imes, S. A (1978). The imposter phenomenon in high achieving women: Dynamics and therapeutic intervention. Psychotherapy: Theory, Research & Practice, Vol 15(3), 241-247.

Piker, S. (2009) The Sexual Paradox: Men, Women and the Real Gender Gap. Scribner, New York, NY.

Pittman, E. (October 3, 2011) How Emergency Management Is Changing (For the Better). Emergency Management Magazine (p.16-20,72-74)

Scheer, K. (2015) Impostor Syndrome: How I Fool My Bosses, and You Too. Retrieved from Toptal.com

Young, V. (2011). The Secret Thoughts of Successful Women. Crown Publishing, New York, NY.

## About the Author

### Emily Kies

Emily Kies is the Senior Director of Emergency Management at Elgin Community College outside of Chicago, Illinois where she lives with her husband and daughter. She holds her Certified Emergency Manager (CEM®) through the International Association of Emergency Managers. She has a Bachelor of Science in Homeland Security and Emergency Preparedness from Thomas Edison State University in Trenton, New Jersey and is currently pursuing her Master of Business Administration at Columbia Southern University. When she has the time she enjoys reading, horseback riding and running.

# Culture Shift Needed in Cybersecurity Training

Dr. Denise Kinsey
University of Houston

Dr. Jane LeClair
Washington Center for Cybersecurity Research & Development

Dr. Tanis Stewart
Thomas Edison State University

Each year organizations around the globe spend billions of dollars in cybersecurity training. In 2019 the estimated cost will top $124 billion dollars and costs are expected to increase dramatically (Morgan, 2019).  Morgan (2019), writing for *Cybersecurity Ventures,* notes that "…global spending on cybersecurity products and services will exceed $1 trillion cumulatively over the five-year period from 2017 to 2021" (p.1). Despite this vast expenditure of resources cyber breaches continue to occur and cost organizations huge amounts of time, money, and resources. According to a recent article in *Security Magazine* (2019), "Cybercriminals exposed 2.8 billion consumer data records in 2018, costing more than $654 billion to U.S. organizations"(p.1). Barrabi (2019), notes the high cost of an 'average' breach and writes "breaches are even more expensive for US-based firms, which face an average cost of $8.19 million per cyberattack". The projected losses are more than five times expenditures for training.

Since so much is spent on security, yet costly breaches continue to occur, the natural question to ask is 'what has gone wrong?' The answer to that question lies not with additional hardware and software. The fault lies with the failure of organizations to adopt a cultural shift that totally embraces cybersecurity and training that utilizes affective learning as a keystone for increased recall and assimilation. Cultural shift may be defined as a new process or way of doing things that counters the basic and long held beliefs of an organization. It is not an instantaneous event but a gradual change or shift away from the past towards a new and more fruitful path that leads to the anticipated long-range goal. This will require a change not only in how employees think and behave, and it will challenge their long held beliefs.

In far too many cases organizations simply check the 'completed' box in regard to cybersecurity training. Employees at all levels are made to observe a basic awareness training course and sent back to their job. As such, the training is too often taken lightly, treated as just the latest required training initiative, and little actual learning is carried back to the workplace. What is needed is a complete cultural shift in the way the training and education of the workforce is accomplished.

This shift can be accomplished by designing programs that implement affective domain learning as a cornerstone to the employee learning process. This domain is part of the triad known as Bloom's Taxonomy. The triad includes affective, cognitive and psychomotor skills that promote learning. The affective domain is associated with creating an *awareness* of an issue or value that is sought, *reinforcing* behavior that aligns with the new value, *promotion* of the value associated with the change, and finally *defense* of the value that we are seeking to attain.

Utilizing the affective domain in the training at all levels of an organization will result in members having an awareness of the need for the training (implying that there is danger to the organization in not adhering to cybersecurity rules), reinforcing positive behavior (regarding proper cybersecurity hygiene and constantly reinforcing the need for it), promotion by the individual of the value of cybersecurity to others, and defense of the need for security and adherence to cyber policies. At this last level, the members of an organization fully support the need for cybersecurity, support those who also adhere to the rules, and quickly jump to the defense of the need for security, intervening where necessary to prevent violation of the rules that might endanger the integrity of the digital system the organization utilizes. Constructing training focusing on the affective domain that can go beyond receiving knowledge and skills in the cyber arena to valuing and demonstrating behavior change in the realm of cyber hygiene and adherence to cyber policies within the organization. A shift of the entire organizational culture in this area is needed, as it serves as the missing piece of cybersecurity training.

## What Isn't Happening in Cyber Training

Cybersecurity education has evolved considerably over the past years. It began in 2011 when the National Institute for Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) focused on defining the NICE Cybersecurity Workforce Framework (NCWF) providing a common language and a set of tasks and skills required to work in the discipline (Newhouse, Keith, Scribner, and Witte, 2016). The evolution progressed to a joint task force on cybersecurity education (CSEC201) producing guidelines for cybersecurity program development in colleges, universities, and industry-based programs. The guidelines identify six major knowledge areas (KAs): data security, software security, system security, human security, organizational security and societal security with associated topics and sub-topics that can be used when developing training programs (Joint Task Force, 2017). The guidelines focus on the topics and technical skills that that should be taught but do not identify the need to incorporate the affective domain as a focal point for the training.

In today's business environment information security continues to be a major concern. Most organizations, regardless of size, have implemented some form of cybersecurity awareness training for all employees. Each organization's program has some unique qualities depending upon the characteristics and needs of the particular business. There is a wealth of information and resources available to assist companies in addressing security awareness training. Available resources generally include some combination of topics from the knowledge areas identified by the joint task force.

The primary source for training and educating cybersecurity professionals is college and university degree and certificate programs. These programs are housed in business schools, computer science departments, computer engineering departments, criminal justice departments and others because of cybersecurity's multi-disciplinary nature. Cabaj, Domingos, Kotulski, and Respicio (2018), studied cybersecurity programs from a sampling of major universities including Boston University, George Mason University, Johns Hopkins University, New York University, Pennsylvania State University and several schools of the same caliber in various parts of the world. Their study found that the structure of the programs and the content of the courses vary but tend to follow the general framework developed by the joint task force. The study also found that top-ranking schools were making program revisions to follow recent developments in the field (Cabaj et all, 2018). However, there was no indication that course development is incorporating the affective domain so that the learner's attitude, personal values and assimilation of ethical values are goals within the content.

Training can be purchased from any number of organizations that offer pre-developed courses or semi-customized programs. Businesses also have the option of developing their own in-house program. Organizations often seek information on best practices as a gauge for measuring effectiveness of their training. Best practices criteria often focuses on offering training that complies with local and federal laws; including the entire organization in the training process; establishing a required baseline of assessment; creating a system for clear communication about the program; making the training entertaining, enforcing, reviewing and repeating the content; and creating reinforcement and motivation for learning (Secureworks, 2018). Using this criteria, organizations proceed to develop and offer training that includes the topics and sub-topics that have been recommended and are in line with what is happening in the industry. Organizations make sure that all employees complete the training and perhaps offer some simplistic way to see if employees are practicing what they have learned, such as periodically sending out company-generated phishing emails.

In both environments, training for cybersecurity professions, and in the business community the missing component is emphasis on the behavioral aspects of training. The focus is on general awareness of a set of topics offered in the cognitive domain or a series of prescribed or technical steps that may not resemble an actual cybersecurity situation for the psychomotor domain. The learner's attitude, personal values and changing of value structure are not being addressed. Without this inclusion the employee will not make the material part of their habits and attitudes and therefore probably not respond to cybersecurity situations in the desired manner.

## What Can Be Done To Make the Shift Happen?

Cognitive training is valuable when there are terms or aspects that must be memorized and will be used in a manner similar to the initial presentation. Consider terminology of malware attacks to prepare for a multiple-choice exam. This method of training would be effective. If the employee must repeat a series of tasks in a specific order consistently and there is little deviation from the presentation of the situation psychomotor would be an appropriate choice. The need to match the type of training to the domain used for presentation is essential for the success of the training. As cybersecurity awareness training requires employees to recognize a threat that could present in a variety of manners, which could occur in different mediums or platforms, and requires different responses based on the previous two items, it requires a behavior and personality shift compared to other types of training.

As cybersecurity awareness varies from a social engineering attack via a phishing email to someone posing as a legitimate employee or contractor within a facility using a pre-described set of steps is impossible as ‘one-size-fits-all’ is not appropriate. When presented with a phishing email management may want employees to forward the email to the IT department helpdesk or an email account specifically for suspicious emails. Employees sent with an email with an attachment will not simply forward that email if the main source of business for the company is through emails containing attachments. The employee must identify several indicators of phishing or invalidation of the email as a legitimate business communication prior to following the company policy. With the high instance of email hacking and use of sent emails as a means of learning how to communicate impersonating the actual employee, the training must include information on how to identify subtle differences and anomalies to the usual business process.

An unknown person walking through the halls of an organization may not garner much attention but if that person attempts to open the door to the server room there may be a need to confront the individual and ask who they are and where they are going. Asking for proper identification is a legitimate response. Once ‘cleared’ that person may be allowed to proceed but with a chaperone. If the person is not able to validate their presence what should be done? Obviously, the situation should not easily progress to an unknown person wandering the building and policies and procedures should be updated to ensure this does not occur, but if it did, how should the employee respond? Standing in the middle of the building screaming ‘Intruder! Intruder!’ is not necessarily the most effective solution and could incite panic unnecessarily if the person has legitimate reason for being there.

Situational training, as it contains a number of variables and resulting decision tree type options is not for every situation. Consider the ‘Choose your own adventure’ type books many read in their youth. Having some control over the outcome of a story or the main character’s actions was often enjoyable and led to re-reading of the book as there were different potential outcomes based on the choice of the reader. Is that how the nightly news should be delivered? Probably not. In that situation offering the facts in the most succinct manner possible is often preferred.

## Next Steps

Identification of what should be taught, how it should be presented, and how many options should be included is another set of important tasks and another place where such training can easily become overwhelming and tabled until a later date. How many options should be presented? How detailed should the trainers craft each session? How vague must the material be so as to be applicable, yet how specific as to be memorable? These essential questions should be answered early in the process. When it is determined that there is in-house expertise to develop such training how should those developers begin? If there is no in-house expert who can assist? How does an organization successfully identify a subject matter expert or other resource to aid in the development? How often should the training occur? How should learning be assessed? What should be the ramifications for successful or unsuccessful assessment – reward to those who are correct, re-training for those who are unsuccessful? Termination with repeated unsuccessful assessments?

When considering development of cybersecurity awareness training in the affective domain what types of materials or media should be used? One way to introduce trainees to situations and preferred ways to respond is through the use of video clips and multiple technologies (video with visual and audio content) aid in retention of the information as multiple senses are used to learn. Discussions on why the depiction is the best response and inclusion of participants' opinions and reinforcement of that option aid in attendees' assimilation the information. A goal for the training is to have the attendee respond to the information in such a way that it reinforces this value and experience for quick recall if circumstances arise and for integration into their behavior and responses. This is why situational training is more effective than general terminology training. Allowing employees to learn of the necessary response in a situation that closely mimics a possible breach attempt that applies to their job duties will make it more meaningful, relevant, and memorable.

Another essential element for employees to modify their attitudes and adopt the training is for all levels of organizational leadership to exhibit endorsement of the training and shift in culture and for employee tasks and normal operating procedures to be changed to reflect this update. Inclusion of a cybersecurity policy is an essential first step, but beyond that infusing cybersecurity best practices into every other policy and procedure will aid in such modification of behavior.

A cybersecurity policy is essential as it guides the direction of an organization in regard to cybersecurity decisions and planning. The cybersecurity policy must adhere to the organizations' mission and vision to be effective and bring comfort and vision instead of confusion and strife. InfoSec Institute identifies a security policy as essential as it 'is the statement of responsible decision makers about the protection mechanism of a company's crucial physical and information assets' (InfoSec, 2019). The security policy is the high-level document that guides employees and management in decisions as to cybersecurity issues but does not detail the specific items to employ such as a brand or manufacturer. Those decisions should align with the policy but are more detailed and often made by those assigned the specific duties of securing or architecting the corporate network.

SecureWorks (2018), identifies several elements for cybersecurity training and awareness. These elements include how to recognize common hacking attempts and what to do if the employee encounters an attack with spam, phishing, malware including ransomware, and social engineering. Those topics are essential and should be included but how the content is covered can differentiate successful identification and avoidance of an attack or a catastrophic loss to the organization when an attempt was not successfully thwarted. Elevation of the concepts from simple terms to dramatizations – live or recorded- can aid in remembrance of the issue and how to best respond. Watching an attack play out allows employees to identify the various elements of the attack and recognize the areas where the attack could be used against them in their capacity at the organization.

Then what is different between affective domain focused training and creating several videos that employees can watch? The difference is the use of job specific scenarios, including discussion of why a choice is correct or more-correct or less-correct than another as many attacks are a series of smaller contacts and attempts where each could be successful or none could. Effectively tying the elements together and allowing employees to practice the concepts is essential to successful recognition and adherence to company policy when a hack manifests. There are many companies that offer cybersecurity awareness training. Some offer their training to vertical markets, which is often more effective that generalized training as it addresses the employees at companies in a certain area such as restaurants or manufacturing facilities. What is missing from most of these training products is the application to the specific responsibilities of the employee and any dialog as to why a selection of choices is effective in thwarting the attack or what could be done differently if such a situation occurred again as it is often a series of decisions and not a single action that allows an attack to propagate.

Learning why co-workers made one selection over another aids in understanding of the decision and if the training is effective because they did or did not understand what was intended. A type of peer pressure aids in enhancing the importance of making the correct decision. But if an employee initially discards a concept as not useful or unimportant they may re-evaluate the idea when they hear the ideas of their peers. Making the material relevant and memorable are important aspects of the training.

# References

Barrabi, T. (2019, July 23). Here's what data breaches are costing companies in 2019. CyberSecurity FOX Business. Retrieved from https://www.foxbusiness.com/technology/heres-what-data-breaches-are-costing-companies-in-2019

Bloom's taxonomy: the affective domain (2015). Retrieved from http://www.nwlink.com/~donclark/hrd/Bloom/affective_domain.htm

Cabaj, K., Domingos, D., Kotulski, Z., and Respicio, A. (2018). Cybersecurity Education: Evolution of the Discipline and Analysis of Master Programs, Elsevier.

Data breaches cost $654 billion in 2018. (2019, June 4). Security Magazine. Retrieved from https://www.securitymagazine.com/articles/90320-data-breaches-cost-654-billion-in-2018 InfoSec Institute (2019). Introduction to Cyber Security Policy. Retrieved from https://resources.infosecinstitute.com/cyber-security-policy-part-1/#gref

Joint Task Force on Cybersecurity Education, Cybersecurity Curricula 2017, Version 1.0 Report (2017, Dec 31). Curricula Series Joint Task Force on Cybersecurity Education. Retrieved from: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

Morgan, S. (2019, June 10). Global Cybersecurity Spending Predicted to Exceed $1 Trillion From 2017-2021. Retrieved from https://cybersecurityventures.com/cybersecurity-market-report/

Newhouse B, Keith S. Scribner B, Witte G. NICE Cybersecurity Workforce Framework (NCWF), National Initiative for Cybersecurity Education (NICE). Draft NIST special Publication 800-181; 2016. Available from: https://www.nist.gpv/itl/appkued-cybersecurity/nice/resources-workforce-framework

SecureWorks (2018, Nov 12). Cybersecurity Awareness Training: Threats and Best Practices. Retrieved from: https://www.secureworks.com/blog/cybersecurity-awareness-training-best-practices

## About the Authors

### Dr. Denise Kinsey

Dr. Denise Kinsey has consulted in IT and OT cybersecurity for many years including projects in business, manufacturing, financial, medical, nuclear, and ethanol production. Denise's academic career includes her present position as Assistant Professor at the University of Houston, a Carnegie designated Tier I Research School. She has published several books and articles in various cybersecurity topics. She is co-chair of the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) curriculum project. Her relevant certifications include the CISSP, C|CISO, and Security+.

### Dr. Jane LeClair

Dr. Jane LeClair is the President and CEO of the Washington Center for Cybersecurity Research & Development whose mission is to increase knowledge of the cybersecurity discipline. Before assuming her current position, Dr. LeClair was the Chief Operating Officer at the National Cybersecurity Institute (NCI) in Washington, D.C., previously served as Dean of the School of Business and Technology at Excelsior College and had a 20-year career in commercial nuclear power. Dr. LeClair has written and edited numerous books, journals and articles related to cybersecurity, nuclear technology and education and is a staunch advocate for women in technology.

### Dr. Tanis Stewart

Dr. Tanis Stewart is a consultant who focuses on information technology and cybersecurity Awareness. She is fully committed to promoting women in technology and cybersecurity. Dr. Stewart has held numerous industry Information Technology positions including Network Engineer, Vice President of Network Engineering, and Director of Information Technology. She has worked as an adjunct professor and Instructional Designer at several universities in the United States, Europe and Asia.

Book Review

Mack, K, M.; Winter, K; & Soto, M

**Culturally Responsive Strategies for Reforming STEM Higher Education: Turning the TIDES on Inequity**

Bingley, UK: Emerald Publishing Limited, 2019.
ISBN: 978-1-78743-406-6 (Print)
ISBN: 978-1-78743-405-9 (Online)
ISBN: 978-78769-953-3 (Epub)

Dina Thomason
University of Texas at El Paso

## Background

As the population of the United States becomes increasingly diverse, representatives in science and technology must reflect that diversity to create an equitable society for all individuals. Teaching to increase diversity and equity in STEM (TIDES) is a STEM initiative aimed at increasing interest and retention rates of traditionally underrepresented groups in STEM fields. Grant-funded through the Association of American Colleges and Universities (AAC&U), the program targets women and minorities, specifically African-Americans, Latinos, and Native Americans/Alaska Natives.

The TIDES program was introduced into introductory computer science courses at colleges and universities throughout the United States. Computer science was chosen because diversity in the computer sciences was decreasing at the beginning of the project despite an increase in diversity in college admissions. The book, *Culturally Responsive Strategies for Reforming STEM Higher Education: Turning the TIDES on Inequity*, edited by Kelly M. Mack, Kate Winter and Melissa Soto, is a compilation of papers from institutions that implemented TIDES strategies into their computer science courses after receiving professional development training and support in culturally sensitive teaching practices.

The editors begin the anthology by discussing the historical context of TIDES and the disparity between the number of new computer science jobs created annually in the United States (120,000) and the number of computer science undergraduate degrees awarded each year (56,000). This discrepancy is complicated by the new demographics of college students; women and minority groups are the new majority in colleges and universities, but there is a lack of culturally sensitive pedagogy in computer science education that encourages women and minorities to enter computer science fields. Underrepresented groups provide a crucial perspective in solving technological and scientific problems, and pedagogy in computer science must attempt to enrich teaching methods in order to develop and promote their talents. To remain globally competitive and to create a more democratic society, technology professions in the United States must reflect the people they represent.

## Participants

The nineteen schools that participated in the TIDES program were as diverse as the student populations they were trying to reach. Included were small liberal arts colleges (Fairleigh Dickenson University, Pitzer College and Westminster College), larger public universities (Wright State University, Queens College and California State University at Northridge) and traditionally black or women's colleges (Morgan State University, Fayetteville State University, and Byrn Mawr College). TIDES participants developed campus-based programs in computer sciences that broke from traditional Eurocentric teaching methods by using instructional strategies that were culturally relevant to learners of diverse backgrounds. This included acknowledging the cultural significance of students' backgrounds and connecting the curriculum to students' prior knowledge and cultural understandings. Faculty connected curriculum and modes of instruction as *organizers* by creating spaces that affirmed students' backgrounds, as *mediators* by helping students identify contradictions like equality, and as *orchestrators* by making students' learning compatible with traditional frames of reference. Three representatives from each university attended TIDES institutes that exposed them to the social science behind cultural responsiveness, forcing them to challenge their assumptions about students' abilities based on gender, race or socioeconomic background. Besides the yearly institutes and workshops, institutional support was provided through online portals and discussions. Participating institutions in three year period accumulated over 200 hours interacting with socially and culturally relevant pedagogical ideas and literature including topics on justice, bias, equity and white fragility.

## Major Themes

### *Culturally Responsive Teaching (CRT)*

Each individual institution participating in TIDES wrote their own set of objectives, but a primary goal of TIDES was to effect a professional development program that created spaces for faculty to recognize their own personal biases, and to better understand how their biases and traditional modes of teaching prevented them from creating an inclusive atmosphere that validated the experiences of all students. At the University of Dayton (UD), a private Catholic school with a predominantly white student body, the project began with concerns regarding the faculties willingness to change their pedagogical approach.  The school had made some attempts to attract more diversity into their programs, but had not fully analyzed which programs were successful and which weren't. For the first year of the TIDES program at UD, a Creative Media Applications course was created to address the obstacles underrepresented students faced in persisting in computer science classes. Throughout the first year, pedagogy encouraged collaboration through a multi-disciplinary approach. In the second year of the TIDES program the instructor allowed the students to choose their own topic of study around the theme of social justice. Throughout the projects, instructors used accessible programming languages, and just-in-time supports to help students' develop their programming skills.  After engaging in the three year-long program, faculty felt they had more sensitivity in responding to their students' individual cultural experiences. The goals for UD of improving student diversity and engagement in STEM disciplines aligned with the TIDES program, and through curricular changes and faculty development, by the end of the TIDES grant, surveys showed that faculty felt more comfortable implementing more culturally relevant pedagogy by allowing more collaboration and student choice, and promoting greater social cohesion by creating student working groups.

Similar results were found at other institutions. At Morgan State University (MSU), a public university with a predominantly African-American student body, the goal through the TIDES program was to integrate Computational Data Science (CDS) tools into the curriculum and to enable faculty to incorporate culturally sensitive teaching into their practice. To increase students' interest in computer science and to prepare students for the workplace, MSU revised their STEM curriculum and created a Computational Data Sciences Certificate Program. To address the need for culturally responsive teaching, MSU implemented more student-centered learning and student led discussions as well as created apprenticeships and designed projects that built on students' prior knowledge and experiences. After their participation in the three year TIDES program, faculty responses on surveys were positive and faculty felt empowered to integrate culturally responsive teaching into their classrooms. At Fayetteville State University (FSU), another historically black university, only two of the twenty-nine math and computer science faculty members were American born at the start of the TIDES program causing cultural misunderstandings. One of the goals at FSU for the TIDES project was to increase culturally responsive teaching to create more effective curriculum. To that end, faculty designed culturally relevant projects integrating computer programming into music, video games and robotics. Student satisfaction with instruction measured through faculty evaluations had higher scores. On a scale of 1-5, satisfaction with faculty was 4.33 in the year before TIDES, but rose to 4.45, 4.47 and 4.43 in the three years of TIDES implementation. Faculty participation in TIDES encouraged curriculum redesign, and enabled teachers to appreciate students' cultural differences.

### *Student Recruitment and Retention*

The TIDES project at The University of Puerto Rico at Humacao (UPRH) focused on overcoming stereotypes in computer science. Specifically, the project was aimed at female students from low-income households. The methods used included an outreach program for middle and high school students, professional development for faculty in culturally responsive strategies and changes to the curriculum including focusing more on women in science and supplemental programming workshops. Results were positive and showed a 10% increase in female students entering majors in computational fields at the end of the three year participation in TIDES. Additionally, the outreach program impacted more than 2,000 high school students.

At California State University, Northridge (CSUN), before TIDES was implemented, 32.4% of the student population were underserved minority (URM) women, but the computer science department was comprised of only 6.3% URM women. One of the goals of the TIDES program was to use music to reach culturally diverse students in a beginning computer science course. After the three year period women in TIDES courses had an 11% higher pass rate than those in the control course and all courses redesigned through TIDES had a higher percentage of students earning a C or better than students in the control group.

Institutions that were part of the TIDES program also saw better retention of students in computer science majors. At Montgomery College, a diverse community college in Maryland, a recommendation from the Closing the Achievement Gap Task Force was to "address the academic success, retention, and completion of African-American and Latino students" (p. 155). One strategy implemented was a survey to not only assess students' perception of STEM fields, but also to give background information of the students that faculty could use to make adjustments to their teaching. By including questions on students interests, work schedules and prior learning experiences, faculty used resources to better address the needs of the students including using a flipped classroom model, adjusting faculty office hours to better accommodate student schedules and providing shared electronic resources that provided faculty strategies and teaching tips in culturally responsive pedagogies. Results showed an increase in the number of female, African-American, and Hispanic students majoring in computer science during the three years of TIDES implementation.

Wright State University (WSU) had previously implemented a retention program, SCALE-UP, initially used to increase success in physics courses through collaboration. The results of this program encouraged them to seek further resources through TIDES. Their TIDES program focused on retention of students from Computer Science I to Computer Science II. WSU used a flipped classroom model wherein students viewed lectures and completed readings outside of class, and class time was used for active learning activities. These activities allowed faculty to help students build a computer scientist identity and combat imposter syndrome, or the feeling some students might have that they are not competent. In the first year of TIDES collaboration, WSU was able to increase the level of students able to progress from Computer Science I to Computer Science II with the highest increases (over 50%) seen by a TIDES trained project investigator.

*Student Perceptions*

One of the barriers to success for women and URMs in STEM related fields is the perception students have of their own ability to be successful in STEM fields. Oftentimes students think that STEM fields are not for them because they do not see individuals from similar backgrounds working in STEM. Also, if students see other students with more programming experience they might think they are behind and won't see themselves as able to compete. Though Title IX prohibits discriminating recruitment on the basis of gender, if a discipline has limited involvement by one gender, the school can employ additional recruitment strategies to target a specific gender. This allowed Queens College (QC) to control registration by limiting male enrollment in an introductory computer science course. Once the enrollment reached 50% male, additional males were put on a waiting list. By targeting recruitment efforts towards females, they were able to increase female enrollment to over 40% of the class. Results did not find women changing their majors to computer science after taking the course, but in the classes with controlled registration, women outperformed the men with passing rates of 81% compared to 77% for men. More women were exposed to computer science throughout the three year participation in TIDES, and like the University of Puerto Rico and Humacao, QC formed partnerships with community groups like Girls Who Code and Black Girls Code and area schools to encourage greater participation in computer science fields.

Byrn Mawr's TIDES goals were to develop a scientific computational course for science majors, and to educate faculty about barriers diverse students may have to learning in STEM fields. In faculty workshops, research on underrepresented groups in higher education was introduced, and factors that prevented these groups from being successful in STEM fields was discussed, including imposter syndrome. The computational methods course developed included modules with features like a scientist profile, intended for students to find scientists they could relate to as sources of inspiration, and a term project that allowed students to apply computation to an area of personal interest. The intention of students relating to scientists was not always met as some students in the pilot year of the program chose white, male scientists to profile. Reflection suggests that diversity in science fields must be made explicit. Faculty needs to engage in discussions about bias in the computing industry and why there is a failure to recognize contributions from underrepresented groups.

**Conclusions**

The TIDES program supports institutions dedicated to promoting equity in STEM fields by implementing culturally sensitive pedagogical strategies and developing curriculum to make computer science accessible to underrepresented minorities and women. By providing thoughtful professional development with ongoing support, TIDES has transformed the way institutions approach students. Rather than faculty finding students lacking in skills or not prepared to tackle difficult subject matter, teachers are learning to be more inclusive and design curriculum that adapts to the unique needs of the students. Faculty buy-in is key; without acknowledging the bias they bring into the classroom, teachers cannot begin to engage in culturally responsive pedagogies. Realizing that students need student-centered collaborative activities with ongoing support from faculty and peer mentors is an essential aspect to making computer science more accessible to all students.

Best practices emerging from the TIDES program include using a flipped classroom model to allow more student-directed and student-centered learning to occur during class time (Wright State University), allowing student choice to make learning relevant (Morgan State University, Montgomery College), peer mentoring programs (Morgan State University, California State University, Northridge), community outreach programs (University of Puerto Rico, Humacao, Queens College), and using just-in time supports (University of Dayton). Westminster College had used another best practice, learning communities, for first year students prior to TIDES, but through TIDES developed computer science learning communities for first year students.

The final chapter of the book "Measurement and Assessment" discusses the impact TIDES had on institutions, faculty and students. Over the three-year period, TIDES impacted 276,229 students with 26 new courses taught, 140 courses were redesigned and 83 modules created. The results are significant and moving forward TIDES will continue to support inclusivity in STEM fields. There is also still a need for long term data that would show more underrepresented minorities and women choosing to pursue STEM majors and enter STEM fields. Although perceptions changed for both faculty in how to reach students and students in their ability to be successful in computer science courses, there continues to be a need to retain and recruit underserved minorities in computer science. The institutions participating in TIDES were committed to achieving diversity and equity for their students, but most of those institutions had a diverse student body to work with and they had support from the majority of the faculty. The challenge now is to employ culturally sensitive pedagogy throughout STEM disciplines and to make all universities welcoming to all students. Additionally, more universities need to use strategies to recruit diverse and underrepresented minority students into their undergraduate STEM programs.

## About the Author

### Dina Thomason

Dina Thomason is an educator with over 20 years of experience teaching science, math, and engineering in public and private schools. She currently teaches biomedical science and forensic science at Canutillo High School in El Paso, Texas and is pursuing a doctorate degree from the University of Texas at El Paso in Teaching Learning and Culture with a focus on STEM education.