

Andrew William Green, Ph.D.

[✉ andygreen.phd](mailto:andygreen.phd) [in AndyGreenPhD](https://www.linkedin.com/in/AndyGreenPhD) [GitHub AndyGreenPhD](https://github.com/AndyGreenPhD) [@AndyGreenPhD@infosec.exchange](https://twitter.com/AndyGreenPhD)

Education

- PhD** **Nova Southeastern University**, Information Systems, Supporting Area of Emphasis — Fort Lauderdale, Florida
— Information Security May 2020
- **Dissertation:** [SNS Use, Risk, and Executive Behavior](#)
 - **Advisor:** James Parrish, Ph.D.
 - **Committee Members:** Jason B. Thatcher, Ph.D.; James N. Smith, DBA
- MS** **Kennesaw State University**, Information Systems, Supporting Area of Emphasis — Kennesaw, Georgia
Information Security Jan 2007
- BS** **Kennesaw State University**, Information Systems, Supporting Area of Emphasis — Kennesaw, Georgia
Information Security Jan 2005

Academic Positions

- Kennesaw State University**, Assistant Professor of Information Security and Assurance Kennesaw, Georgia
Aug 2020 – present
- Kennesaw State University**, Full Graduate Faculty Kennesaw, Georgia
Apr 2020 – present
- Kennesaw State University**, Career Coach, Hughes Leadership Program Kennesaw, Georgia
Jan 2017 – Aug 2020
- Kennesaw State University**, Lecturer of Information Security and Assurance Kennesaw, Georgia
June 2012 – Aug 2020
- Kennesaw State University**, Temporary Instructor Kennesaw, Georgia
Aug 2011 – May 2012
- Kennesaw State University**, Temporary Instructor Kennesaw, Georgia
Jan 2010 – Aug 2011
- Kennesaw State University**, Adjunct Instructor Kennesaw, Georgia
Aug 2008 – Dec 2009

Professional Positions

- Strategic Security Consulting Services**, Owner Mar 2020 – present
- Green Consulting**, Owner Mar 2002 – Mar 2020
- Medquist**, Software Developer Sept 1998 – Mar 2002

Publications

Unpacking digital transformation – Constructing a framework based on industry use cases

July 2025

Based on industry use cases, we identify six distinct types of digital transformation (DT), each grounded in a specific concept or enabling technology. These DT types can be implemented individually or combined to drive transformation initiatives. While deploying a single DT type often focuses on improving operational efficiency or streamlining existing workflows, initiatives that combine multiple DT types tend to pursue more ambitious goals, such as the creation of new products, services, or business models. However, the complexity increases significantly with the integration of multiple DT types, as organizations must not only address behavioral changes but also overcome technical challenges involving systems integration, data architecture, and interoperability.

Saeed, Khawaja Asjad, Green, Andrew William, Hedrick, Alison Brooke

[10.1016/j.jik.2025.100759](https://doi.org/10.1016/j.jik.2025.100759) (Journal of Innovation & Knowledge)

What does ChatGPT Know about Information Systems?

Apr 2025

Large language models such as ChatGPT provide efficient access to a wealth of information. However, there are significant questions regarding the depth and quality of knowledge in any one domain. This paper focuses specifically on the information systems (IS) field and assesses ChatGPT's knowledge. To analyze the extent and quality of information systems knowledge derived from queries to ChatGPT, we used over 3,000 queries from a broad range of exam and quiz questions. These queries were obtained from university courses and professional information system certification exams. The query topics are based on a framework for information systems education, with queries gathered from multiple faculty members at different universities. The results of querying ChatGPT with these questions find that ChatGPT can answer 65% to 85% of information systems queries successfully, across each of the areas of the framework. ChatGPT performed well on essay, true/false and multiple choice questions, with no statistical difference between its success rate on multiple choice and true/false questions. We conclude that ChatGPT tends to perform approximately at the level of an average student, but may not perform at a level sufficient to pass certain professional exams. ChatGPT's knowledge is very broad, covering virtually all areas of the information systems knowledge we identified, but not at an expert level.

O'Leary, Daniel E., French, Aaron M., Storey, Veda C., Buckman, Joseph R., Chua, Cecil, Green, Andrew William, Gu, Grace, Niederman, Fred, Pereira, Francis, Templeton, Gary, Wallace, Linda

[10.17705/1CAIS.05619](https://doi.org/10.17705/1CAIS.05619) (Communications of the Association for Information Systems)

To report or not to report? Extending Protection Motivation Theory to Vulnerability Discovery and Disclosure

July 2024

Vulnerability researchers face difficult choices when considering whether to reporting a finding to an organization with which they are unaffiliated. We used components of Protection Motivation Theory (PMT) to create the Vulnerability Discovery and Disclosure (VDD) model to understand the decision-making processes of vulnerability researchers. PMT uses high fear appeals, threat appraisals, and coping appraisals to encourage employee prosocial behaviors while VDD proposes low fear and threat with high coping, to encourage reporting. In this exploratory study, we surveyed active vulnerability researchers to gain insight into their concerns when deciding to report to an organization. Using principal components analysis, we developed and refined the VDD survey, which may be tested by future researchers. We also discovered a higher-order efficacy construct, comprised of response and self-efficacy. We theorize that well-developed vulnerability disclosure policies, in line with a low-fear, low-threat appraisal and high efficacy may establish a culture of trust between organizations and vulnerability researchers, encouraging more reports.

Green, Andrew William, Oliver, DeJarvis, Woszczyński, Amy B.

[10.1016/j.cose.2024.103880](https://doi.org/10.1016/j.cose.2024.103880) (Computers & Security)

Jan 2024

Principles of Network Security

Principles of Network Security offers a comprehensive, approachable, and up-to-date foundation for teaching network security to students in high school, trade school, or college-level courses. This textbook introduces core concepts in network security, cryptography, secure architecture, threat analysis, and monitoring while addressing modern challenges like IoT, cloud security, AI, and Zero Trust frameworks. Each chapter combines foundational theory with real-world examples and current best practices. The book emphasizes practical knowledge across layered topics, from the OSI and TCP/IP models and data communication protocols to firewall configuration, VPN deployments, wireless network protections, and access control models. It includes coverage of leading standards and frameworks from NIST, CIS, and ISO. Rich pedagogical features - such as learning objectives, review questions, hands-on exercises, and short projects - help reinforce key skills and prepare students for further study or entry into cybersecurity roles. Whether used in a semester-long survey or as a base for certification pathways, this textbook equips students with the knowledge they need to navigate the complexities of modern network security.

Green, Andrew William, Whitman, Michael E., Mattord, Herbert
he.kendallhunt.com/product/principles-network-security (Kendall Hunt Publishing)

Aug 2023

Analysis of Honeypots in detecting Tactics, Techniques, and Procedures changes based on IP Address

The financial and national security impacts of cybercrime globally are well documented. According to the 2020 FBI Internet Crime Report, financially motivated threat actors committed 86% of reported breaches, resulting in a total loss of approximately \$4.1 billion in the United States alone (Federal Bureau of Investigation, 2022). In order to combat this, our research seeks to determine if threat actors change their tactics, techniques, and procedures (TTPs) based on the geolocation of their target's IP address. To answer this research question, we will construct a honeypot network distributed across multiple continents to collect attack data from geographically separate locations concurrently. We will configure the honeypots to offer vulnerable services and collect log data from the services for analysis. This approach will allow us to aggregate log data about attacks against specific services commonly targeted by threat actors. After we complete data collection, we will analyze the data to gain insight into the TTPs used by the threat actors. The analysis will use collected attack data attributes such as IP origin, service type, and executables delivered along with other transport layer analysis techniques to provide metadata on threat actor TTPs. Once the analysis is complete, we will have a greater insight into threat actor activities and produce a list of items that firms can use to monitor, protect, and maintain their environments and to detect attacks earlier, along with taking appropriate defensive action to lessen or eliminate the risk associated with these attacks.

Reynolds, Carson, Green, Andrew William
aisel.aisnet.org/treos_amcis2023/1 (Americas Conference on Information Systems (AMCIS))

Analysis of Honeypots in detecting Tactics, Techniques, and Procedures changes based on IP Address

The financial and national security impacts of cybercrime globally are well documented. According to the 2020 FBI Internet Crime Report, financially motivated threat actors committed 86% of reported breaches, resulting in a total loss of approximately \$4.1 billion in the United States alone (Federal Bureau of Investigation, 2022). In order to combat this, our research seeks to determine if threat actors change their tactics, techniques, and procedures (TTPs) based on the geolocation of their target's IP address. To answer this research question, we will construct a honeypot network distributed across multiple continents to collect attack data from geographically separate locations concurrently. We will configure the honeypots to offer vulnerable services and collect log data from the services for analysis. This approach will allow us to aggregate log data about attacks against specific services commonly targeted by threat actors. After we complete data collection, we will analyze the data to gain insight into the TTPs used by the threat actors. The analysis will use collected attack data attributes such as IP origin, service type, and executables delivered along with other transport layer analysis techniques to provide metadata on threat actor TTPs. Once the analysis is complete, we will have a greater insight into threat actor activities and produce a list of items that firms can use to monitor, protect, and maintain their environments and to detect attacks earlier, along with taking appropriate defensive action to lessen or eliminate the risk associated with these attacks.

Reynolds, Carson, Green, Andy

digitalcommons.kennesaw.edu/undergradsymposiumksu/spring2023/presentations/341
(KSU Undergraduate Symposium)

Sept 2022

Social Networking Continuance and Success: A Replication Study

The success of social networking sites relies on members' continuous use. We replicate a study evaluating the relationship of continued-use intention to the success of social networking sites to determine whether the results obtained with a US sample can be generalized to the South Korean context. Using two culturally distinct samples, we demonstrate limitations to the generalizability of the original study's findings and important constructs influencing continued-use intention across cultural boundaries.

French, Aaron M., Green, Andrew William

[10.1080/08874417.2022.2119443](https://doi.org/10.1080/08874417.2022.2119443) (Journal of Computer Information Systems)

Jan 2020

Responding to Cybersecurity Challenges: Securing Vulnerable U.S. Emergency Alert Systems

U.S. emergency alert systems (EASs) are part of the nation's critical infrastructure. These systems are built on aging platforms and suffer from a fragmented interconnected network of partnerships. Some EASs have an easily identifiable vulnerability - their management website is available via the Internet. Authorities must secure these systems quickly. Other concerns exist, primarily the lack of policies for reporting vulnerabilities. To begin an assessment of U.S. EASs, we used Shodan to evaluate the availability of these websites in six southeastern states. We found 18 such websites that were accessible via the Internet, only requiring user credentials to login to the system. Next, we searched for published policies on the reporting of vulnerabilities; we found no vulnerability disclosure policies for any of the systems identified. To identify, prioritize, and address EAS vulnerabilities, we present a list of technical and management strategies to reduce cybersecurity threats. We recommend integrated policies and procedures at all levels of the public-private-government partnerships, along with system resilience, as lines of defense against cybersecurity threats. By implementing these strategies, U.S. EASs will be positioned to update critical infrastructure, notify groups of emergencies, and ensure the distribution of valid and reliable information to the populations at risk.

Green, Andrew, Woszczyński, Amy B., Dodson, Kelly, Easton, Peter

[10.17705/1CAIS.04608](https://doi.org/10.17705/1CAIS.04608) (Communications of the Association for Information Systems)

Zombies, Sirens, and Lady Gaga – Oh My! Developing a Framework for Coordinated Vulnerability Disclosure for U.S. Emergency Alert Systems

U.S. emergency alert systems (EAS) run on legacy software with aging hardware and limited cybersecurity. While EASs are an essential component of the U.S. critical infrastructure, they are often under-funded, and workers frequently lack the knowledge to protect these systems adequately. Recent compromises of various EASs have not inspired public confidence. We present a method for EAS authorities to engage with external cybersecurity researchers to find, recover from, and disclose vulnerabilities using coordinated vulnerability disclosure (CVD) policies. Clearly written CVD policies set guidelines and legal bounds for cybersecurity research, taking advantage of researcher expertise while working to strengthen the cybersecurity of the patchwork public-private-government networks comprising EASs. We intended to investigate the CVD policies of EASs in seven southeastern states; however, we could find no CVD policies through the entire supply chain. Instead, we investigated the CVD policies of the top 10 technology firms on the Fortune 500 list, analyzing best practices in terms of publication of a CVD policy, as well as: setting eligibility requirements, describing the submission process, delineating researcher restrictions, outlining agreements on sharing credit, and explaining bounties (if relevant). We recommend that EAS authorities develop CVD policies in line with suggested criteria, using policies from top technology organizations combined with the proposed framework, and using cybersecurity researchers as a valuable component of the EAS supply chain.

Woszczynski, Amy, Green, Andrew, Dodson, Kelly, Easton, Peter
[10.1016/j.giq.2019.101418](https://doi.org/10.1016/j.giq.2019.101418) (Government Information Quarterly)

Nov 2017

Learning Outcomes for Cyber Defense Competitions

Cyber defense competitions (CDCs) simulate a real-world environment, where the competitors must protect the information assets of a fictional organization. These competitions are becoming popular at the high school and college levels, as well as in industry and governmental settings. However, there is little research to date on the learning outcomes associated with CDCs or the long-term benefits to the participants as they pursue future educational, employment or military goals. For this exploratory research project, we surveyed 11 judges and mentors participating in a well-established high school CDC held in the southeastern United States. Then we developed a set of recommended learning outcomes for CDCs, based on importance of the topic and participant preparedness for future information-security related endeavors. While most previous research has focused on technology issues, we analyzed technological, human, and social topics, to develop a comprehensive set of recommendations for future CDCs.

Woszczynski, Amy B., Green, Andrew
www.jise.org/Volume28/n1/JISEv28n1p21.html (Journal of Information Systems Education)

Jan 2014

Principles of Incident Response and Disaster Recovery

PRINCIPLES OF INCIDENT RESPONSE & DISASTER RECOVERY, 2nd Edition presents methods to identify vulnerabilities within computer networks and the countermeasures that mitigate risks and damage. From market-leading content on contingency planning, to effective techniques that minimize downtime in an emergency, to curbing losses after a breach, this text is the resource needed in case of a network intrusion.

Whitman, Michael E., Mattord, Herbert J., Green, Andrew
www.cengage.com/c/principles-of-incident-response-and-disaster-recovery-2e-whitman/
 9781111138059 (Cengage Learning)

Addressing Emerging Information Security Personnel Needs. A Look at Competitions in Academia: Do Cyber Defense Competitions Work?

Aug 2013

This paper is part of a proposed study that looks at the emerging information security personnel needs of organizations. We are attempting to explore the correlation between components of a regional cyber defense competition and an organization's needs in terms of employing adequately trained information security personnel. We look to identify some unique characteristics of a regional academic cyber defense competition via the critical success factors method.

Green, Andrew, Zafar, Humayun

aisel.aisnet.org/amcis2013/ISSecurity/RoundTablePresentations/5 (Americas Conference on Information Systems (AMCIS))

Guide to Network Security

Jan 2013

GUIDE TO NETWORK SECURITY is a wide-ranging new text that provides a detailed review of the network security field, including essential terminology, the history of the discipline, and practical techniques to manage implementation of network security solutions. It begins with an overview of information, network, and web security, emphasizing the role of data communications and encryption. The authors then explore network perimeter defense technologies and methods, including access controls, firewalls, VPNs, and intrusion detection systems, as well as applied cryptography in public key infrastructure, wireless security, and web commerce. The final section covers additional topics relevant for information security practitioners, such as assessing network security, professional careers in the field, and contingency planning. Perfect for both aspiring and active IT professionals, GUIDE TO NETWORK SECURITY is an ideal resource for students who want to help organizations protect critical information assets and secure their systems and networks, both by recognizing current threats and vulnerabilities, and by designing and developing the secure systems of the future.

Whitman, Michael E., Mattord, Herbert J., Mackey, David, Green, Andrew

www.cengage.com/c/guide-to-network-security-1e-whitman (Cengage Learning)

Hands-on Information Security Lab Manual

Jan 2013

HANDS-ON INFORMATION SECURITY LAB MANUAL, Fourth Edition, helps you hone essential information security skills by applying your knowledge to detailed, realistic exercises using Microsoft Windows 2000, Windows XP, Windows 7, and Linux. This wide-ranging, non-certification-based lab manual includes coverage of scanning, OS vulnerability analysis and resolution, firewalls, security maintenance, forensics, and more. The Fourth Edition includes new introductory labs focused on virtualization techniques and images, giving you valuable experience with some of the most important trends and practices in information security and networking today. All software necessary to complete the labs are either available online as a free download or included in the accompanying CD, making it easy to plan and complete lab work. An ideal resource for introductory, technical, and managerial courses or self-study, this versatile manual is a perfect supplement to the PRINCIPLES OF INFORMATION SECURITY, SECURITY FUNDAMENTALS, and MANAGEMENT OF INFORMATION SECURITY books.

Whitman, Michael E., Mattord, Herbert J., Green, Andrew

www.cengage.com/c/guide-to-network-security-1e-whitman (Cengage Learning)

Jan 2012

Guide to Firewalls and VPNs

Firewalls are among the best-known network security tools in use today, and their critical role in information security continues to grow. However, firewalls are most effective when backed by thoughtful security planning, well-designed security policies, and integrated support from anti-virus software, intrusion detection systems, and related tools. GUIDE TO FIREWALLS AND VPNs, THIRD EDITION explores firewalls in the context of these critical elements, providing an in-depth guide that focuses on both managerial and technical aspects of security. Coverage includes packet filtering, authentication, proxy servers, encryption, bastion hosts, virtual private networks (VPNs), log file maintenance, and intrusion detection systems. The text also features an abundant selection of realistic projects and cases incorporating cutting-edge technology and current trends, giving students the opportunity to hone and apply the knowledge and skills they will need as working professionals. GUIDE TO FIREWALLS AND VPNs includes new and updated cases and projects, enhanced coverage of network security and VPNs, and information on relevant National Institute of Standards and Technology guidelines used by businesses and information technology professionals.

Whitman, Michael E., Mattord, Herbert J., Green, Andrew

www.cengage.com/c/guide-to-firewalls-and-vpns-3e-whitman/9781111135393 (Cengage Learning)

Aug 2007

Management of Security Policies for Mobile Devices

This paper is part of a proposed study that looks at the emerging information security personnel needs of organizations. We are attempting to explore the correlation between components of a regional cyber defense competition and an organization’s needs in terms of employing adequately trained information security personnel. We look to identify some unique characteristics of a regional academic cyber defense competition via the critical success factors method.

Green, Andy

[10.1145/1409908.1409933](https://doi.org/10.1145/1409908.1409933) (Information Security Curriculum Development Conference (InfoSecCD))

Institutional Service

Kennesaw State University , Member, Coles College Faculty Review Committee (CFRC)	Kennesaw, Georgia May 2026 – present
Kennesaw State University , Vice Chair, Information Technology Advisory Committee (ITAC)	Kennesaw, Georgia Jan 2026 – present
Kennesaw State University — Coles College of Business , Committee Member, Evening MBA Curriculum Review Committee	Kennesaw, Georgia Oct 2025 – May 2026
Kennesaw State University — Department of Information Systems and Security , Co-chair, Faculty Search Committee — Assistant Professor of Information Systems and Security	Kennesaw, Georgia May 2025 – Mar 2026
Kennesaw State University — Coles College of Business , Director, KSU Cyber Range at Coles College	Kennesaw, Georgia Mar 2024 – present
Kennesaw State University , Faculty Advisor, Orthodox Christian Fellowship (OCF)	Kennesaw, Georgia Aug 2022 – present
Kennesaw State University — Department of Information Systems and Security , Program Coordinator, Information Security and Assurance (ISA) Undergraduate Program	Kennesaw, Georgia Aug 2015 – Aug 2026
Kennesaw State University , Faculty Advisor, KSU Offensive Security Research Club (OffSec)	Kennesaw, Georgia Dec 2013 – present

Kennesaw State University , Committee Member, Cybersecurity Governance Committee	Kennesaw, Georgia Aug 2022 – Jan 2026
Kennesaw State University – Department of Information Systems and Security , Committee Member, Retention, Progression, and Graduation (RPG) Committee for IS and ISA Programs	Kennesaw, Georgia Aug 2022 – May 2023
Kennesaw State University – Coles College of Business , Committee Member, Coles Research and Development Council (RDC)	Kennesaw, Georgia Aug 2020 – May 2023
Kennesaw State University – Department of Information Systems and Security , Committee Member, Faculty Search Committee – Assistant Professor of Information Security and Assurance	Kennesaw, Georgia Sept 2020 – May 2021
Kennesaw State University – Department of Information Systems and Security , Committee Chair, BBA–Information Security and Assurance Redesign Committee	Kennesaw, Georgia Aug 2020 – May 2021
Kennesaw State University – Department of Information Systems and Security , Committee Chair, Faculty Search Committee – Clinical Assistant Professor of Information Security and Assurance	Kennesaw, Georgia Apr 2020 – Sept 2020
Kennesaw State University – Department of Information Systems and Security , Committee Member, Department Chair Search Committee – Department of Information Systems	Kennesaw, Georgia Aug 2019 – Mar 2020
Kennesaw State University – Department of Information Systems , Committee Member, Curriculum Committee	Kennesaw, Georgia Jan 2013 – May 2017
Kennesaw State University – Institute for Cybersecurity Workforce Development (ICWD) , Committee Member, Executive Director Search Committee	Kennesaw, Georgia Feb 2017 – Apr 2017
Kennesaw State University – Coles College Center for Information Security Education (CISE) , Assistant Director for Operations	Kennesaw, Georgia Jan 2014 – Apr 2016
Kennesaw State University – Department of Information Systems and Security , Committee Member, Faculty Search Committee – Lecturer of Information Systems	Kennesaw, Georgia Oct 2015 – Dec 2015
Kennesaw State University , Committee Member, University Undergraduate Policies and Curriculum Committee (UPCC)	Kennesaw, Georgia Aug 2012 – Dec 2015
Kennesaw State University – Department of Information Systems and Security , Committee Member, BBA–Information Security and Assurance Curriculum Working Group	Kennesaw, Georgia Aug 2009 – Aug 2015
Kennesaw State University – Coles College of Business , Committee Member, Associate Dean of Undergraduate Programs Search Committee	Kennesaw, Georgia Mar 2015 – July 2015
Kennesaw State University , Faculty Advisor, KSU Information Systems Security Association (ISSA) Student Organization	Kennesaw, Georgia Aug 2012 – Aug 2014

Professional Service

Association for Information Systems (AIS) , President-Elect, Special Interest Group on Information Security and Privacy (SIGSEC)	Aug 2025 – present
BSides Atlanta Conference , Organizer	Atlanta, Georgia Jan 2018 – present

Association for Information Systems (AIS) , Workshop Organizer, SIGSEC Pre-ICIS Workshop	Nashville, Tennessee May 2025 – Dec 2025
Association for Information Systems (AIS) , Track Organizer, Information Security and Privacy Track — Americas Conference on Information Systems (AMCIS)	Montréal, Canada Aug 2020 – Aug 2025
Association for Information Systems (AIS) , At-large Director, Special Interest Group on Information Security and Privacy (SIGSEC)	Aug 2022 – Aug 2025
Association for Information Systems (AIS) , Workshop Organizer, SIGSEC Pre-ICIS Workshop	Bangkok, Thailand May 2024 – Dec 2024
Kennesaw State University, Kennesaw, Georgia , Session Chair, 2024 Dewald Roode Information Systems Research Symposium (DRIS)	Kennesaw, Georgia Oct 2024
Association for Information Systems (AIS) , Track Organizer, Information Security and Privacy Track — Americas Conference on Information Systems (AMCIS)	Salt Lake City, Utah May 2023 – Aug 2024
Association for Information Systems (AIS) , Workshop Organizer, SIGSEC Pre-ICIS Workshop	Hyderabad, India May 2023 – Dec 2023
Association for Information Systems (AIS) , Session Chair, 29th Americas Conference on Information Systems (AMCIS)	Panama City, Panama Aug 2023
Association for Information Systems (AIS) , Track Organizer, Information Security and Privacy Track — Americas Conference on Information Systems (AMCIS)	Minneapolis, Minnesota Jan 2022 – Aug 2022
Association for Information Systems (AIS) , Session Chair, 28th Americas Conference on Information Systems (AMCIS)	Minneapolis, Minnesota Aug 2022
Association for Information Systems (AIS) , Track Organizer, Information Security and Privacy Track — 26th Americas Conference on Information Systems (AMCIS)	Salt Lake City, Utah Jan 2020 – Aug 2020
Association for Information Systems (AIS) , Session Chair, 26th Americas Conference on Information Systems (AMCIS)	Salt Lake City, Utah Aug 2020
Association for Information Systems (AIS) , Track Organizer, Information Security and Privacy Track — 24th Americas Conference on Information Systems (AMCIS)	New Orleans, Louisiana Jan 2018 – Aug 2018
Information Systems Security Association (ISSA) , Board Member (non-voting) — Metro Atlanta Chapter	Atlanta, Georgia Jan 2014 – Dec 2014
Association for Computing Machinery (ACM) , Program Committee Member, Southeast Conference	Tuscaloosa, Alabama Jan 2012 – Mar 2012

Awards and Honors

- 2026:** Named "Influential Instructor" by Graduating Students — Kennesaw State University
- 2025:** AIS Distinguished Member
- 2025:** Named "Influential Instructor" by Graduating Students — Kennesaw State University
- 2023:** "Five in Flight" Alumni Award for Outstanding Service — Coles College of Business, Kennesaw State University
- 2022:** Named "Influential Instructor" by Graduating Students — Kennesaw State University
- 2020:** Named "Influential Instructor" by Graduating Students — Kennesaw State University
- 2019:** Named "Influential Instructor" by Graduating Students — Kennesaw State University
- 2018:** Named "Influential Instructor" by Graduating Students — Kennesaw State University
- 2017:** Named "Influential Instructor" by Graduating Students — Kennesaw State University
- 2016:** Named "Influential Instructor" by Graduating Students — Kennesaw State University
- 2016:** Innovation in Teaching Award — Coles College of Business, Kennesaw State University
- 2016:** Gary Roberts Outstanding Advisor to Student Organizations Award — Coles College of Business, Kennesaw State University
- 2015:** Named "Influential Instructor" by Graduating Students — Kennesaw State University
- 2014:** Named "Influential Instructor" by Graduating Students — Kennesaw State University
- 2014:** Gary Roberts Outstanding Advisor to Student Organizations Award — Coles College of Business, Kennesaw State University
- 2012:** Named "Influential Instructor" by Graduating Students — Kennesaw State University
- 2011:** Named "Influential Instructor" by Graduating Students — Kennesaw State University