
Kevin A. Barton, Ph.D.
Instructional Associate Professor
Computing & Cyber Security
College of Business

kbarton@tamusa.edu

Academic Background

Ph.D. Nova SouthEastern University.

M.S. Our Lady of the Lake University.

B.B.A. Nova Southeastern University.

Other Texas Central College.

Professional Certifications

Offensive Security Certified Professional (OSCP), 2020, San Antonio, TX.

AccessData Certified Examiner, 2010

Certified Information System Security Professional (CISSP), 2006, Clearwater, FL.

CompTIA Security+, 2006

Skills

Expertise

Information security, cyber security, computer forensics, computer networks, penetration testing. Working in teams. Supervising and motivating personnel from diverse backgrounds.

Work Experience

Work Experience

Instructional Associate Professor in Computer Information Systems, Texas A&M-San Antonio (September, 2013 - Present), San Antonio, Texas. Instructed courses in telecommunications, information security, computer security, and network security. Administered computer information systems laboratory. Lead contact for university for NSA/DHS designation as Center of Academic Excellence-Cyber Defense Education (CAE-CDE). Prepared and submitted CAE-CDE redesignation in 2016. Chaired adjunct faculty search committee, College of Business Curriculum Committee (2020-2021). Department representative on University Faculty Senate (2016 and 2019-2021). Member University Curriculum Committee (2015 and 2020-2021). Developed and managed course in Blackboard learning management system. Incorporated video conferencing systems such as Webex, Zoom and Blackboard Collaborate to deliver synchronous online courses. Developed course materials including labs and class exercises to provide interactive, hands-on learning using multiple virtualization technologies. Virtualization technologies include Docker, Vagrant, VMware & Oracle Virtual Box, and Google Cloud Computing.

Assistant Professor Non-Tenure Track of Computer Information Systems and Security, Our Lady of the Lake University (August, 2008 - August, 2013), San Antonio, Texas. Instructed courses in information security, computer and network security, information systems technology, networking, and computer forensics and investigations. Advised students. Member of Information Technology Committee, Portal Governance Committee, and chaired or participated on employee search committees. Developed and managed course in Blackboard learning management system.

Director, Center for Information Assurance Management & Leadership, Our Lady of the Lake University (August, 2008 - August, 2013), San Antonio, Texas. Directed NSA Center for Academic Excellence in Information Assurance and Education. Developed and implemented community outreach. Collaborated with business, government, and other academic institutions on information security issues.

Adjunct Faculty, Our Lady of the Lake University (May, 2008 - August, 2008), San Antonio, Texas. Develops and

delivers curriculum and manages classroom and schedule for Masters of Science in Computer Information Systems and Security, Information Assurance.

Director, Information Assurance, Department of the Army (March, 2008 - August, 2008), San Antonio, Texas. Senior installation Information Assurance Manager; oversaw IA actions of 60 IA professionals and network/system administrators supporting over 10,000 users and 7,000 hosts. Developed and enforced IA policies and procedures. Led incident response, determined appropriate actions and coordinated with Army Computer Emergency Response Team and Theater Network Operations and Security Center. Prepared installation's secure and unclassified networks for certification and accreditation under the Defense Information Assurance Certification and Accreditation Process.

Director, Information Assurance and Configuration Manager, Department of Defense (May, 2005 - March, 2008), San Antonio, Texas. Senior IT Configuration Management Specialist and technical field expert for the Tri-Service Infrastructure Management Program Office (TIMPO) that manages Department of Defense (DoD) Military Health System (MHS) communications and computing infrastructure (C&CI). Developed configuration management policies and plans. Developed and executed program management office incident response plan. Managed enterprise ports, protocols and services; developed and executed certification and accreditation program; established service level agreements for computer network defense. Implemented information assurance vulnerability management program and host based security system. Executed \$10.2 million budget providing hardware and software maintenance and sparing, supporting enterprise with over 74,000 network infrastructure assets at 260 military medical treatment facilities. Coordinated government depot and private industry support to ensure flexible and cost effective sparing and maintenance program. Considered technological changes and advances to develop and execute upgrade and technical refresh plans ensuring network infrastructure met operation, security and supportability requirements. Submitted requests for proposals and evaluated contractor bids. Evaluated, prioritized and initiated IT acquisition efforts to meet MHS C&CI infrastructure maintenance, sparing and technical refresh requirements. Served as a alternate project leader and performed oversight of contract performance. Chaired C&CI Disaster Recovery Planning Working Groups; led development of enterprise disaster recovery plan. Briefed supervisors, senior leaders and service representatives on program status and initiatives.

Telecommunications Senior Advisor, U.S Air Force, Headquarters US Air Forces Europe (March, 2001 - August, 2004), Ramstein AB, Germany. Established strategic direction, developed policy, and managed manpower and personnel actions for 1,490 electronic maintainers at 39 locations in Europe. Created, reviewed, and edited executive correspondence; published maintenance policy. Determined manning priorities and skill utilization for emergency and contingency operations. Evaluated and submitted changes to manpower assessment standards; utilized manpower standards to determine most effective and efficient distribution of manpower resources. Directed development of formal training capabilities, implemented new courses. Assisted unit leaders throughout Europe to resolve complex policy, manpower, and personnel issues; trusted by leaders for making well researched, fair, and proper decisions. Provided functional expertise during development of AF-wide manpower measurement tools. Chaired boards to select individual, work center, and unit level awards; participated on AF central awards boards; edited three individual and one unit award that won AF level in 2003.

Telecommunications/Information-Technology Manager, U.S. Air Force, Misawa Cryptologic Operations Center (September, 1999 - March, 2001), Misawa AB, Japan. Led 170 military, civilian and contractor personnel operating and maintaining state-of-the-art telecommunications and computer equipment valued at \$85 million. Evaluated individual/work center performance; developed controls to improve efficiency/quality. Oversaw project management for approximately 60 computer system upgrades per year. Coordinated with other base organizations to ensure civil engineering, test equipment calibration/repair, security, supply, and other support functions met mission requirements. Assisted in developing and executing \$360K operation and maintenance budget. Controlled scheduled/short-notice maintenance on antenna systems from Alaska to South Korea. Motivated subordinates, produced over 15 quarterly, annual, and professional military education award winners.

Satellite Systems Maintenance Manager, US Air Force, Misawa Cryptologic Operations Center (February, 1997 - September, 1999), Misawa AB, Japan. Planned and programmed equipment upgrades; justified and awarded \$14 million to upgrade satellite radio frequency distribution system. Supervised four work centers and 38 technicians installing and maintaining satellite systems, data processors, and a full range of fixed and tracking antennas. Recognized as Air Intelligence Agency Lt General Leo Marquez award winner, 1998, the command's best Communication-Electronics Maintenance Supervisor-Manager of the year. Managed engineering services contract; drafted Request For Proposals and Statement of Work; evaluated proposals and participated in award of new contract and transition between contractors. Developed and executed branch budget; authorized contract purchases up to \$25,000. Reviewed quality control reports to identify trends; implemented corrective action.

Consulting Experience

2021: Brass, Inc, Vulnerability Remediation, Consulted on incident response following a cyber attack against the company.

2014: VTS, Vulnerability Remediation, Network hardening and malware clean-up.

2013: VTS, Incident Response, Incident response and server recovery.

2013: Glorietta Camps, Network Design, Telecommunications and network design.

Teaching

Teaching Activities

Student Assign-Independent Studies

2013 - *Student internship*. 1 student.

2013 - *Student internship*. 1 student.

2009 - *Independent study*. 3 students.

Student Assign-Students Advised (UG)

2012 - *Student Advising, Spring 2012*. 17 students.

2011 - *Student Advising, Fall 2010*. 20 students.

2011 - *Student Advising, Spring 2011*. 20 students.

2010 - *Student Advising Spring 2009*. 18 students.

2010 - *Student Advising, Fall 2010*. 17 students.

2009 - *Student Advising, Spring 2009*. 17 students.

2009 - *Student Advising, Fall 2009*. 17 students.

Intellectual Contributions

5 year Intellectual Contributions Grid

Category	Total
Articles in Refereed Journals	1
Books, Monographs, Compilations, Manuals, Supplements, Chapters, Cases, Readings	1
Presentations of Non-Refereed Papers	1
Other Research, Non-refereed	1

Refereed Articles

Kock, N., Moqbel, M., Barton, K. A., & Bartelt, V. (2018). Intended continued use social networking sites: Effects on Job Satisfaction and Performance. *International Journal of Virtual Communities and Social Networking*, 8 (2), 28-46, doi: 10.4018/IJVCNS.2016040103.

Barton, K. A., Tejay, G., Lane, M., & Terrell, S. (2016). Information system security commitment: A study of external influences on senior management. *Computers & Security*, 59, 9-25, doi: 10.1016/j.cose.2016.02.007.

Chapters, Cases, Readings, Supplements

Kock, N., Moqbel, M., Barton, K. A., & Bartlet, V. (2018). Intended continued use social networking sites: Effects on job satisfaction and performance. In Information Resources Management Association (Ed.), *Social issues in the workplace: Breakthroughs in research and practice* (pp. 472-493). Hershey, PA: IRSA.

Refereed Proceedings

Tejay, G. P., & Barton, K. A. (2013). Information System Security Commitment: A Pilot Study of External Influences on Senior Management. *46th Hawaii International Conference on Systems Science(HICSS 46)*.

Barton, K. A., & Jeffries-Horner, C. J. (2012). Database Intrusion Detection: Defending Against the Insider Threat. *Americas Conference on Information Systems*.

Presentations of Refereed Papers

National

Barton, K. A. & Tejay, G. P. (2013). *Information System Security Commitment: A Pilot Study of External Influences on Senior Management*. 46th Hawaii International Conference on Systems Science(HICSS 46), Wailea, Hawaii.

Barton, K. A. & Horner, C. J. (2012). *Database Intrusion Detection: Defending Against the Insider Threat*. Americas Conference on Information Systems., Seattle, Washington.

Presentations of Non-Refereed Papers

State

Barton, K. A. (2018). *Developing Cyber Security Muscle Memory through Active Learning*. Invited presentation at 2018 Conference on Cyber Warfare: Constructing an Effective Cyber Defense Strategy for the Workforce, Laredo, Texas.

Grants

Research

2014: Barton, K. A., Trippey, M., & Burdwell, R., U.S. Air Force Asian Office on Aerospace Research and Development (AOARD), Principal Investigator, GOV-Air Force Office of Scientific Research (AFOSR).

2013: Barton, K. A. & Trippey, M., Asian Office of Aerospace Research and Development research grant., Principal Investigator, GOV-Air Force Office of Scientific Research (AFOSR).

2013: Jeffries-Horner, C. J. & Barton, K. A., SBE: Small: Senior Management Participation in Information System Security and Fair Information Practices: An Empirical Study on Impact to Regulatory Controls, Co-Investigator, GOV-National Science Foundation (NSF).

Teaching

2014: Hewitt, B. & Barton, K. A., CyberCorps: Scholarship for Service, Co-Investigator.

2013: Jeffries-Horner, C. J. & Barton, K. A., CyberCorps: Scholarship for Service, Co-Investigator.

Other Research

2019: Barton, K. A., *Elements of Anti-Phishing Training: A Comparative Literature Review*. Article review for Computers and Security.

2016: Barton, K. A., *Experiential Based Learning in a Cloud-based Cyber Security Lab: Integration with: NICE CyberSecurity Framework*.

This project develops Cyber Security and Forensics Experiential Based Learning (EBL) for Texas A&M University-San Antonio (TAMU-SA) Computer Science (CS) and Computer Information Systems (CIS) students through management of and interaction with a cloud-based computing lab. JagCloud is an IaaS cloud-based computing environment for CS/CIS students to complete a wide range of computing labs. JagCloud will support student development through two student development paths, academic courses and JagCloud student management teams. JagCloud enhances A&M University-San Antonio's (TAMU-SA) ability to deliver Computer Information System and Computer Science programs, including cyber defense programs, to remote students using active learning methods. CS/CIS students will be exposed to JagCloud through coursework beginning in their first academic year. Students will also play pivotal roles in governance, development and operation of JagCloud. Student participation in the various management roles of JagCloud will be through courses, student organizations and student employment.

The purpose of this grant is to develop the course content and faculty supervisory processes to implement JagCloud development paths. Course content will include JagCloud instructional material for students, lab virtual machines and instructions, and assessments. Supervisory processes will include the supporting roles needed to guide, direct and assess student participation on the JagCloud management teams. The NICE Cybersecurity Workforce Framework will be used as the model to develop student knowledge, skills, and abilities through both development paths.

As a result, TAMU-SA will graduate students with enhanced Cyber Security and Forensics experience. The professional Cyber and information security industry seeks graduates who are equipped with skills and practice, rather than knowledge alone.

2016: Barton, K. A., *Reviewer for Computers & Security: Network Moving Target Defence (sic) Technique Based on Collaborative Mutation*.

Service

Service to the Institution

Department Assignments

Faculty Sponsor:

2019-2020: Collegiate Cyber Defense Competition Coach/Sponsor

2017-2018: Student Cyber Organization

2017-2018: Information Systems Security Association Student Chapter

2015-2016: Student Cyber Organization

Member:

2020-2021: Department of Computing and Cyber Security Curriculum Committee

Department Assignments

Member:

2021-2022: Department of Computing and Cyber Security Curriculum Committee

2019-2020: Department of Computing and Cyber Security Faculty Search Committee

Mentoring Activities:

2019: Aggies Invent - A&M-SA Competition

Department Assignments

Mentoring Activities:

2016-2017: Information Systems Security Association Student Chapter

Department Assignments

Other Institutional Service Activities:

2020-2021: Coach, Collegiate Cyber Defense Competition

College Assignments

Member:

2019-2020: College Faculty Meetings

2019-2020: Bylaws Committee

2018-2019 – 2019-2020: Computing and Cybersecurity Faculty Meetings

2018-2019: College Faculty meetings

2018-2019: NTT faculty evaluation committee

College Assignments

Chair:

2020-2021 – 2021-2022: College of Business Curriculum Committee

2019: College of Business Task Force on Curriculum Delivery

College Assignments

Member:

2017-2018: College of Business Faculty Qualifications Committee

2016-2017: College of Business Faculty Workload Committee

2016-2017: College of Business Curriculum Committee

College Assignments

Member:

2021-2022: College of Business Strategic Planning Committee

University Assignments

Committee Chair:

2012-2013: Learning Organization

University Assignments

Committee Member:

2019-2020: COVID 19 Faculty Senate Task Force

University Assignments

Committee Member:

2015-2016 – 2016-2017: Faculty Awards Committee

2015-2016 – 2016-2017: Faculty Senate

2015-2016: Curriculum Committee

University Assignments

Committee Member:

2018-2019 – 2020-2021: Faculty Senate

2018-2019: Faculty Senate Ad Hoc Committee on Faculty Pay and Summer Teaching

University Assignments

Committee Member:

2011-2012: Strategic Planning Core Team

2010-2011: Portal Implementation Committee

2010-2011: Portal Governance Committee

University Assignments

Committee Member:

2020-2021 – 2021-2022: Undergraduate Curriculum Committee

University Assignments

Other Institutional Service Activities:

2016-2017: Application for Center of Academic Excellence in Cyber Defense Education

2011-2012: Application for Center of Academic Excellence in Information Assurance Education

Thesis Assignments

Member:

2021-2022: Thesis Committee Member

Service to the Profession

Academic Conference: Panelist

2018: 2018 Conference on Cyber Warfare: Constructing an Effective Cyber Defense Strategy for the Workforce, Laredo, Texas (State). Panelist on cyber security education

2018: 2018 Cybersecurity Education Conference, San Antonio, Texas (State). Member of Present and Future

Cybersecurity Best Practices, student faculty and education panel question session.

Reviewer - Article / Manuscript

- 2020: A Semi-Automated Forensic Investigation Model for Online Social Networks. Article review for Computers & Security (International).
- 2020: A Semi-Automated Forensic Investigation Model for Online Social Networks. Article review for Computers & Security (International).
- 2020: Computers & Security: A Cross-Cultural Investigation of Information Security Awareness (International).
- 2020: Computers & Security: Investigating the Effect of Security and Privacy on IoT Device Purchase Behavior. (International).
- 2020: Computers & Security: Indicators for Maturity and Readiness for Digital Forensic Investigation in Era of Industrial Revolution 4.0. (International).
- 2020: Computers & Security: Investigating the effect of security and privacy on IoT device purchase behavior (International).
- 2019: Computers & Security: A Complex Network-Based Critical Node Identification Method for Industrial Control Systems Using Range of Failure Impacts (International).
- 2019: Computers & Security: Malicious Host Identification Using Machine Learning Classification in Cloud Forensics. (International).
- 2019: Computers & Security: A Supervised Learning Approach for Characterization and Classification of Socialbot Targets in Twitter (International).
- 2019: Computers & Security: Susceptibility to Phishing on Social Network Sites: A Personality Information Processing (PIP) Model (International). (International).
- 2019: Computers & Security: Can Employees' Neutralizations be Overcome? A Field Experiment on Password Policy. (International).
- 2019: Computers & Security: Automated, Real-Time Risk Analysis Model (International).
- 2018: Computers & Security: A Method of Adaptive Protection from False Information in Computer Networks rev1. (International).
- 2018: Computers & Security: Can Employees' Neutralizations be Overcome? A Field Experiment on Password Policy rev 1. (International).
- 2018: Computers & Security: Explaining the Privacy Paradox - A systematic review of literature investigating privacy attitude and behavior rev 2. (International).
- 2018: Computers & Security: Explaining the Privacy Paradox - A systematic review of literature investigating privacy attitude and behavior rev 1. (International).
- 2017: Computers & Security: Explaining the Privacy Paradox - A systematic review of literature investigating privacy attitude and behavior (International).
- 2017: Computers & Security: Does Cybersecurity Policy Awareness Affect Employees' Cybersecurity Behavior? An Exploratory Analysis rev 1. (International).
- 2017: Computers & Security: Inadvertent Disclosures of Inventions in Social Media Affecting Patent Rights rev 1 (International).
- 2017: Computers & Security: Does Cybersecurity Policy Awareness Affect Employees' Cybersecurity Behavior? An Exploratory Analysis (International).
- 2017: Computers & Security: Correlating Human Traits and Cybersecurity Behavior Intentions (International).
- 2017: Computers & Security: The significance of information security monitoring and other social learning factors on employees' security assurance behaviour (International).
- 2017: Computers & Security: Inadvertent Disclosures of Inventions in Social Media Affecting Patent Rights (International).
- 2017: Computers & Security: Understanding Organizational Citizenship Behavior regarding Information Security (OCB-S): A Leadership Approach Perspective rev 1 (International).
- 2017: Computers & Security: Network Moving Target Defence Technique Based on Collaborative Mutation rev 3

(International).

2017: Computers & Security: Understanding Organizational Citizenship Behavior regarding Information Security (OCB-S): A Leadership Approach Perspective (International).

2017: Computers & Security: Can Employees' Neutralizations be Overcome? A Field Experiment on Password Policy (International).

2017: Computers & Security: Network Moving Target Defence (sic) Technique Based on Collaborative Mutation rev 2 (International).

2017: Computers & Security: Network Moving Target Defence (sic) Technique Based on Collaborative Mutation rev 1. (International).

2017: Computers & Security: τ -Safety: A Privacy Model for Sequential Publication with Arbitrary Updates rev 1 (International).

2017: Computers & Security, A Methodology and Experimental Environment for Analysing Ransomware (International).

2016: Computers & Security: Network Moving Target Defence (sic) Technique Based on Collaborative Mutation (International).

2016: Computers & Security: The Influence of Academic Degree on CISSP Exam Takers (International).

2016: Computers & Security: On Data Leakage from Non-production Systems (International).

2016: Computers & Security: Performance Analysis of the impact of DDoS attacks on Web Services - A Realtime Investigation (International).

2016: Computers & Security: A Privacy-preserving Cancelable Iris Template Generation Scheme using Decimal Encoding and Look-up Table Mapping (International).

2016: Computers & Security, On Data Leakage from Non-production Systems (International).

2016: Computers & Security, The Influence of Academic Degree on CISSP Exam Takers (International).

2016: Computers & Security, A Network Moving Target Defense Technique Based on Collaboration Mutation (International).

2016: Computers & Security, τ -Safety: A Privacy Model for Sequential Publication with Arbitrary Updates (International).

2016: Computers & Security: A Privacy-preserving Cancelable Iris Template Generation Scheme using Decimal Encoding and Look-up Table Mapping (International).

Reviewer - Grant Proposal Related to Expertise

2013: National Information Assurance Education and Training Program (National). Wrote application for NSA/DHS designation as a Center of Academic Excellence in Information Assurance Education for Our Lady of the Lake University. Designation was awarded for 2012-2017.

Other Professional Service Activities

2020: 2020 CAE in Cybersecurity Symposium, Online, Virtual (National).

2019: Enigma 2019 Industry Conference, Burlingame, California (National).

2015 – 2016: Southwest Collegiate Cyber Defense Competition (Regional). Organize and execute SWCCDC competition.

2014: Southwest Collegiate Cyber Defense Competition (Regional). Organize and execute SWCCDC competition.

Reviewer: Ad Hoc Reviewer for a Journal

2022: Computers & Security: SCADA Vulnerabilities and Attacks: A Review of the State-of-the-Art and Open Issues (International).

2022: Computers & Security: Espoused organizational and team culture values as antecedents of protection motivation among IT employees (International).

2021: Computers & Security: Cloud Computing Security: A Survey on Service-based Models (International).

2021: Computers & Security: Cloud Computing Security: A Survey on Service-based Models (International).

2021: Computers & Security: Behavioural Monitoring and Security Profiling in the Internet of Things (IoT)

(International).

2021: Computers & Security: An Empirical Analysis of the Information Security Culture Key Factors Framework (International).

2021: Computers & Security: Chronological Sail Fish Optimizer for preserving privacy in cloud based on kathirao product (International).

2021: Computers & Security: An Empirical Analysis of the Information Security Culture Key Factors Framework (International).

2021: Computers & Security: Indicators for Maturity and Readiness for Digital Forensic Investigation in Era of Industrial Revolution 4.0 (International).

Service to the Community

Speech / Presentation at a Community Meeting

2017: Cyber Talk Radio, 2017: Cyber Talk Radio, Episode 42, Cybersecurity Program at Texas A&M-San Antonio, July 15, 2017,

Professional Development

DS: Research-Related Conference/Seminar

2019: Enigma 2019. Enigma centers on a single track of engaging talks covering a wide range of topics in security and privacy. Our goal is to clearly explain emerging threats and defenses in the growing intersection of society and technology, and to foster an intelligent and informed conversation within the community and the world. We view diversity as a key enabler for this goal and actively work to ensure that the Enigma community encourages and welcomes participation from all employment sectors, racial and ethnic backgrounds, nationalities, and genders. Read this blog post about Enigma's commitment to diversity, written by Enigma 2019 Program Co-Chairs Ben Adida and Franziska Roesner.

2018: Americas Conference on Information Systems..

Other Professional Development

2019: CodePath Security Tech Fellow Training. Completed CodePath Tech Fellow training in preparation for delivering the A&M-SA course in partnership with the Facebook Security program.

Professional Seminars / Workshops

2019: WebEX Training. College of Business WebEX training.

Technology-Related Training

2018: Penetration Testing with Kali Linux.

Using information gathering techniques to identify and enumerate targets running various operating systems and services

Writing basic scripts and tools to aid in the penetration testing process

Analyzing, correcting, modifying, cross-compiling, and porting public exploit code

Conducting remote, local privilege escalation, and client-side attacks

Identifying and exploiting XSS, SQL injection, and file inclusion vulnerabilities in web applications

Leveraging tunneling techniques to pivot between networks

Creative problem solving and lateral thinking skills

Last updated by member on 03-Feb-22 (09:47 AM)