Robin “Montana” Williams, CWDP
(702) 743-7143
montana.williams@gmail.com

SUMMARY

- Proven instructor classroom/online experience: information/cyber security, aviation operations, & psychology
- Instructs operationalized cybersecurity risk, compliance, policy development, security & governance operating plan development & implementation within organizations to increase cyber resilience via university program
- Provided subject matter expertise on instructional design of Western Governors Univ cybersecurity program
- Proven track-record—15+ years’ leadership in info technology (IT) security, risk, governance, training & policy
- Experienced Chief Information Security Officer (CISO) consultant built robust security programs from scratch
- Versed in development and implementation of key performance indicators (KPI), cybersecurity risk management principles based on SOX, HIPAA, PCI, CoBiT, ITIL, ISO 27000, NIST 800-53, FISMA, GDPR, GLBA, & NIST NCF
- Globally-recognized cyber education, training, & awareness training expert—built the nation’s training model Solid technical understanding of enterprise security solutions—SaaS, PaaS, IDS/IPS, SEIM, SAP, cloud, & threat intel
- Experienced Cyber Red Team Leader—designed key vulnerability processes to evaluate organizational security functions, assessed enterprise organizations, consulted on security & policy improvement
- Master of relationship building—successfully lead integration of technology, personnel, and architectures to increase global cyber resilience—10+ years’ experience as executing consultant-related activities, author & presenter on cybersecurity solutions to public & private sector senior executives and C-Suite leaders world-wide
- Experienced team & consensus builder, continually mentors to grow individual skills, responsibilities, & leadership
- Instructing operationalized cybersecurity risk, compliance, policy, security & governance, at the university level
- Well recognized, strong national reputation in cybersecurity community—public, private, academic sectors
- Oversaw creation of nation’s cyber workforce framework & developed today’s security training & awareness policy

RELATED QUALIFYING EXPERIENCE

Classroom and Online Instructor Experience—California State University-San Bernardino

- Spring Quarter 2020: IST 511—Cyber Defense (36 students)
  - *Advanced study of information assurance and security including methods and practices used by federal and state agencies, and private sector best practices. Topics include threat assessment, red teaming methods, countermeasures, practices and law. Students will work in simulated environments and will investigate crimes and experience various security scenarios.*
- Spring Quarter 2020: IST 490—Information Systems Planning & Policy (2 Sections—44 students)
  - *This course examines cybersecurity as a business imperative through the eyes of the information security professional/manager/leader not the technologist. Simply, cybersecurity is an organizational risk management function. The primary objective of the class is to teach students how to examine the process of integration of cybersecurity as a primary component of an organizations’ risk management strategy.*
- Winter Quarter 2020: IST 490—Information Systems Planning & Policy (2 Sections—74 students)
- Fall Quarter 2019: IST 309—Information Systems & Technology (41 Students)
  - *Built upon modern information technology, this course is designed to introduce the knowledge and fundamentals underlying the design, implementation, control, evaluation, and strategic/secure use of modern, computer-based information systems for business data processing, office automation, information reporting, and decision-making.*
- Fall Quarter 2019: IST 490—Information Systems Planning & Policy (2 Sections—72 students)
- Spring Quarter 2019: IST 490—Information Systems Planning & Policy (37 students)
- Winter Quarter 2019: IST 511—Cyber Defense (23 students)
- Fall Quarter 2018: IST 490—Information Systems Planning & Policy (38 students)
- Winter Quarter 2018: IST 215—Information Systems Security Professional (36 Students)
  - *This course prepares future security systems managers by transforming the students’ computer skills into business problem solving skills. The student completing this course will be able to identify and execute common exploits, harden systems, and develop sound policies to protect the organization. Students will also be prepared for the CompTIA Security + exam (SY0401) and the 9 domains of Testout Security Pro. The CompTIA Security + certification is globally recognized and is the most sought after entry-level certification across government and industry.*
- Fall Quarter 2017: IST 490—Information Systems Planning & Policy (38 students)
- Spring Quarter 2017: IST 215—Information Systems Security Professional (35 Students)
- Winter Quarter 2017: IST 215—Information Systems Security Professional (34 Students)
- Fall Quarter 2017: IST 490—Information Systems Planning & Policy (30 students)
- Spring Quarter 2016: IST 490—Information Systems Planning & Policy (35 students)
- Winter Quarter 2016: IST 490—Information Systems Planning & Policy (34 students)

- Fall Quarter 2015: IST 215—Information Systems Security Professional (44 Students)
- Fall Quarter 2015: IST 490—Information Systems Planning & Policy (46 students)
- Spring Quarter 2015: IST 490—Information Systems Planning & Policy (33 students)
- 2002-2010: Psychological Operations Instructor, USAF
    - *Taught influence operations, social engineering methodology, human behavior to Cyber Red Team Operators and Leaders*
- 1996-2002: Combat Flight Instructor, USAF
    - *Taught all aspects of military flight operations—theory, planning, operational execution, weapons delivery, combat force integration*

EDUCATION

NorthCentral University, Prescott Valley, AZ—**PhD/ABD, Industrial Organizational Psychology**

Louisiana Tech University, Ruston, LA--**Master's Degree, Industrial Organizational Psychology**

Moorhead State University, Moorhead, MN—**Bachelor's Degree, History**

PUBLICATIONS/ARTICLES

Rauch, D. & Williams, R.B. (2015, Fall). Social Engineering: The Root of the Cyber Threat. *United States Cybersecurity Magazine, 3*(9), 30-34. Retrieved from https://www.uscybersecurity.net/csmag/social-engineering-the-root-of-the-cyber-threat/

Williams, R. B. (2013). *National Initiative for Cybersecurity Education: Best practices for planning a cybersecurity workforce*. Retrieved from https://niccs.us-cert.gov/sites/default/ files/documents/files/Best%20Practices%20for%20 Planning%20a%20Cybersecurity%20Workforce_062813_v4.2_FINAL_NICE%20branded_0.pdf

Williams, R. B. (2013). *National Initiative for Cybersecurity Education: Cybersecurity maturity model—White Paper*. Retrieved from https://niccs.us-cert.gov/sites/default/files/ documents/files/NICE%20Capability%20 Maturity%20 Model%20white%20paper_ 06282013_FINAL_NICE%20branded_0.pdf

Williams, R. B. (2014). *The path towards cybersecurity professionalization: Insights from other occupations.* Retrieved from https://niccs.us-cert.gov/sites/default/files/documents/files/ The%20Path%20Towards%20Cybersecurity% 20Professionalization_0.pdf

Williams, R. B. (2015). 2015 Advanced Persistent Threat Awareness Study: Third Annual. Retrieved from http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Advanced-Persistent-Threats-Awareness-Study-Results.aspx

Williams, R.B. (2016). *State of Cybersecurity: Implications for 2016*. Retrieved from http://www.isaca.org/cyber/ Documents/state-of-cybersecurity_res_eng_0316.pdf

Williams, R. B. (2016). *Arming Organizations to Detect and Respond to Stealthy APTs*. In D. Swanson (Ed.), *The EDP Audit, Control, and Security Newsletter, 53* (5), 7-13. Philadelphia, PA: Taylor & Francis

Williams, R.B. (2018, Summer). Tackling the Gorilla: The C-Suites Role in Cyber Risk. *United States Cybersecurity Magazine, 6*(20), 44-46. Retrieved from https://www.uscybersecurity.net/csmag/tackling-the-gorilla-the-c-suites-role-in-cyber-risk/

QUALIFYING EXPERIENCE

June 2019 – Present: VP, Business Resilience Operational Risk Officer, Wells Fargo, Las Vegas, NV

- Leads results-driven operational risk (e.g., incident management/cyber resiliency) oversight for $104B company
- Evaluates incident response/management, cybersecurity, & crisis communications programs, processes, & technology for 273K+ employees worldwide--serves as organizational leader for related remediation oversight
- Authors credible challenges, documents root causes, tracks front line issue management closure, & remediation plans, to comply with regulatory guidance & industry-best practices across eight financial center lines of business

- Hand-picked as WF's independent risk management SME for organizational cyber resiliency, responsible for development of key processes to ensure oversight, monitoring, & credible challenge of resiliency functions

Mar 2015 – Present: Co-Founder & Managing Partner, Titan Rain Cybersecurity, LLC, Las Vegas, NV

- Co-Founder & Managing Partner—provides virtual Chief Information Security Officer services & consulting services (e.g., policy, technology, programs, training, & risk to Fortune 500 firms) generates $2M annual revenue
- Designed a global cybersecurity training & certification program—certified 1,092 cyber pros from entry-expert
- Cybersecurity/Risk Consultant—provided numerous industry sector solutions related to (e.g., IT/Cybersecurity technology & programs, risk, policy, governance, compliance (GDPR, SOX, NIST CSF, FFIEC, CCPA)
- Provides crypto-currency consulting on secure financial transactions—in order to gain/maintain PCI compliance
- Engagement-focused client relationship-based consulting on global cyber risk management & training to Canada, UK, Sweden, Israel, Czech Republic, Germany, United Arab Emirates, Australia, China, Singapore, & Japan
- **Key Roles:**
  - **Jan 2020 – Present: vCISO Service, Madison Square Garden/TAO Entertainment Grp, Link Tech, Las Vegas, NV**
    - Provides information security consulting services—creating cyber strategy, risk management program, staff models
    - Conducting cyber resiliency review, assessing security program current state, developing future state, & gap analysis
    - Creating a board-level cybersecurity dashboard to communicate current state of information security program
  - **Mar 2018 – Present: Executive Cyber On-Demand Independent Consultant/vCISO, Protiviti, Inc, NY, NY**
    - Provides virtual Chief Information Security Officer (CISO) services and Executive Cybersecurity Consulting to Protiviti, Inc's global Fortune 500 customers—solved their toughest cyber & risk issues—creating resiliency
    - Delivers business-driven information security program consulting—infused security, business continuity, crisis communications, incident response, & regulatory requirements (NYDFS, CCPA, SOX, PCI-DSS, GDPR, HIPAA)
    - Created/employed IT/cyber risk management dashboard—to prioritize key measurements/enhance decision-making
    - Led multiple table-top exercises validating organizational incident response plans to potential cyber threats
  - **Mar 2018 – March 2019: Interim Chief Information Security Officer/Consultant, Everi, Inc., Las Vegas, NV**
    - Chief Information Security Officer (CISO)—built security program & analytical team from ground up—added key technical solutions, created industry recognized policy/procedure best practices, directed 4 security assessments, & overhauled SOX/PCI/GDPR/NYDFS/COSO/GBLA/NIST CSF controls to meet compliance requirements
    - Designed & developed--world's first endpoint security solutions for financial services industry cash transactions; resulting in secure, compliant, & manageable card data environment (PCI-DSS) processing $23B/year transactions
    - Built first corporate cybersecurity, governance, risk, and compliance (e.g., PCI, CCPA, NYDFS) programs—implemented Office 365 security; integrated Mimecast, Jazz Networks Insider Threat Management, file integrity & vulnerability management, app security; crafted risk-based incident response/disaster recovery plans
    - Constructed cyber framework driven business processes to reduce risk & enable $23B/annual card transactions
    - Created best business practices & enhanced operations employing advanced IT methodology through integration of network management tools to enhance confidentiality, integrity, accessibility—78% improvement
    - Identified & resolved remote financial transactions vulnerabilities—built endpoint solutions for untrusted networks
    - Identified network degradation root causes—eliminated duplicative systems; streamlined policy/improved visibility
    - Oversaw project management efforts on multiple IT-related projects—SPLUNK integration, Microsoft 365 Enterprise, data center migration, endpoint security software suite, & a untrusted network firewall deployment
  - **Aug 2016 – Feb 2018: Various Short-Term Consulting Venues, Numerous Global Locations**
    - vCISO services, info security workforce development, info security strategic planning, & cybersecurity tool integration
  - **Apr 2015 – Jul 2016: Senior Cybersecurity Practices Consultant, ISACA, Rolling Meadows, IL**
    - Provided interim consulting services to develop the world's first performance-based cybersecurity certification
    - Conducted & published numerous cybersecurity workforce development articles, papers, threat, & risk studies
    - Analyzed global business needs to enhance cyber workforce skill development to create go-to-market strategies

Mar 2015 – Present: Adjunct Professor, California State Univ-San Bernardino, San Bernardino, CA

- Collegiate professor/researcher of network security & cybersecurity risk—to date taught 573 students in the areas of cybersecurity, risk mitigation, access/network management, incident response, regulatory policy & governance
- Specialized instruction includes: Industry recognized frameworks (CoBIT, ITIL, ISO 27000, NIST CSF); & IT & Cybersecurity Risk Assessments providing basics skills to develop gap-closing organizational remediation plans
- Proficient in multi-modal instruction—in person, live virtual, & on-demand online via BlackBoard, Canvas, Moodle

Sep 2011 – Mar 2015: Chief, Nat’l Cyber Education/Training/Awareness (GS-15), DHS, Washington, DC

- Co-leader & strategic advisor to the President’s National Initiative for Cybersecurity Education (NICE)
- Administered DHS/NSA Centers of Academic Excellence (CAE) program—oversaw development of cyber critical skill education units within 194 CAEs—directed large projects related to academic partnerships with financial, health care, energy, & communications/IT to ensure graduates have the skills to complete job-related tasks
- Supervised DHS team of 8 employees & 28 contractors implementing national cybersecurity awareness, education, training, cyber analytics, & professional development programs & strategy in coordination with 140+ government agencies, 50 states, multiple municipalities, tribal, 7 US territories, & key private sectors companies
- Evaluated 22,000+ gov’t cybersecurity professionals; results identified skill gaps & training needs
- Globally-recognized expert in cyber security role development—architected the nation’s National Cybersecurity Workforce Framework—outlining 32 functional roles & 3,000+ cybersecurity-related knowledge, skills, & abilities (KSAs) in coordination with government, academia, & industry—defined today’s organizational industry standard roles—executed via Presidential Executive Order May 2019 *Strengthening America’s Cybersecurity Workforce*
- Built the backbone of USG cybersecurity learning management system (LMS) for workforce training—Federal Virtual Training Environment/ Cyber Training Events (Fed VTE/CTE) programs; on-demand training & hands-on labs—30K hrs of training per month for 125,000+ federal cyber pros—FY14 saved USG $72M in training costs
- Created the nation’s first cybersecurity knowledge resource (NICCS portal) which provides cyber resiliency tools & opportunities related to education, training, awareness & professional development to 20,000+ visitors/month
- Led policy & standards input for development of tools related to assesses organizational risk exposure & risk tolerance (NIST 800-53 & 800-171); integrated solutions—CDM, SAP, SaaS, IDS/IPS, SEIM, & threat intel
- Oversaw planning & budgeting for $21M USG education & workforce development program budget

Jul 2010 – Sep 2011: Sr. Cyber Intel Tech Pgm Mgr, Nat’l Counter Intel Executive (GS-14), Washington, DC

- Established cyber CI risk assessment process to mitigate insider threats to USG information systems based on FISMA standards—tying user behavior analytics (UBA) modeling based to CMU-CERT Controls & Indicators
- Conducted 7 risk analyses to provide Federal Trade Commission recommendations on global corporate mergers
- Established assessment criteria based on risk exposure & risk tolerance to ensure cyber resilience
- Developed all key knowledge, skill, ability requirements for US cybersecurity counterintelligence mission
- Created/Built cybersecurity analytical team—supports ODNI government counterintelligence assessment mission

Feb 1990 – Jun 2010: Aviator, Operations Officer, Red Team & Unit Commander, USAF, Various Locations

- 8 years’ experience aviation risk monitoring and evaluations—conduct combat readiness evaluations of USAF bomber aircrew members—ensuring crew standardization and operational effectiveness to conduct unit taskings
- Authored USAF’s first cyber training & tactical manual for intrusion detection & offensive defensive tactics
- Directed all operations within the USAF’s only cyber & Information Operations (IO) tactics development organization—supervised 63 military, civilians, & contractors (IT security professionals, analysts & tacticians)
- Directed ops for a 75-person military/civilian division, built AF test/training space & cyber warfare infrastructure
- Led 45-person unit (network, counterintelligence, behavioral scientists, analysts, & security specialists) conducted threat-realistic offensive cyber operations (full-scope red teaming)—trained 167,000+ US/Allied personnel in 2 yrs
- Commanded 57 world-wide cyber red team network & physical security assessments (breach simulations)—8 yrs
    - Conducted counterintelligence (CI) assessments-based threat analysis, technology evaluation, policies & procedures; made recommendations on access control/identification management, awareness training, auditing, configuration management, incident response, personal/physical security, risk & cybersecurity
    - Led team activities conduct all-source threat analysis/production, intelligence fusion (cyber/counter-intel)
    - Successfully penetration testing of all networks—assessed operational cyber risk & compliance posture
    - Consulted w/senior DoD senior leaders/executives driving changes to DoD network infrastructure, training, tactics, techniques, & policy—reduced successful network attacks 95% & saved $2B in 5 years
- Formalized first cyber red team training program; created training plan & courseware; integrated at all organizational levels; built $750K testing & training lab—result: 113 certified red team personnel
- Pioneered non-kinetic effects in AF strategic, operational, & tactical-level exercises; developed scenarios & curriculum; integrated cyber in all combat phases—trained 42,000+ US/coalition forces

- Produced concise technical assessment consultation on adversarial capabilities & integrated results into JTF-GNO’s online annual role-based IT security & education requirements—educated 3.98M DoD personnel
- Increased AF enterprise network resiliency—created AF’s first distance learning curriculum for cyber, social network/media & threat-realistic training; augmented online information assurance training for 777,000+ personnel
- Provided vision & implementation plan--Joint Forces Command’s $20M adversary cyber training range
- Created 5-year/$16M vision/implementation plan for AF flying training range to integrate cyber training
- Designed Air Force’s integrated cyber red team/aggressor program; revised quantitative & qualitative assessment processes; with a limited $1.5M budget—reduced manpower/fiscal requirements 50% & increase mission execution by 100% in 18 months—intro adversarial cyber warfare capabilities in most major coalition exercises

CERTIFICATIONS/PROFESSIONAL DEVELOPMENT

Certified Workforce Development Professional—National Association of Workforce Development Professionals

Certified Information Security Manager (CISM)—ISACA

Certified in Risk and Information Systems Control (CRISC)—ISACA

Certified Computer Network/Info Operations Red Teamer—USAF Information Operations Aggressor Course

Supervisory Leadership Development Program—Department of Homeland Security, Washington DC

Emerging Leaders Program—Central Intelligence Agency, Langley VA

Mentoring Managers/Supervisors Course—Office Director of National Intelligence, Washington DC

Executive Leadership School--Air War College, Maxwell, AFB, AL

Senior Leadership School--Joint Command & Staff College, Norfolk, VA (Information Security Planning Course)

Strategic Planning Training--Joint Doctrine Air Campaign Course, Maxwell AFB, AL

Warfighter, Planning, Integration, & Instructor Training--USAF Weapons School, Nellis AFB, NV

Junior Leadership School--Squadron Officers School, Maxwell AFB, AL

Joint Junior Leadership School—Marine Corps Amphibious Warfare School, Quantico, VA

Instructor/Curriculum Development School—Certified Flight Instructor Course, Barksdale AFB, LA

PROFESSIONAL ORGANIZATIONS

National Assoc of Workforce Development Professionals—Life Member
Veterans of Foreign Wars—Life Member
Society for Industrial Organizational Psychologists
Iraq & Afghanistan Veterans of America—Life Member
Military Officers Assoc of America—Life Member
Armed Forces Comms & Electronics Assoc—Life Member
Sandy Valley Lodge #57, F. A.&M.—Master Mason
York Rite Mason

Air Force Association—Life Member
American Psychological Association
Disabled American Veterans—Life Member
Golden Key International Honour Society
Association of Old Crows
ISACA
Scottish Rite 32º Degree Mason
Shriners’ International

AWARDS/RECOGNITION/OTHER INFORMATION

- ***Retired Lieutenant Colonel, United States Air Force—21 years of service***
- *Decorated combat-veteran* of Operation Allied Force, Operations Enduring & Iraqi Freedom—awarded 25 major medals/ribbons of commendation for service to the United States of America
- Disabled Veteran (Service Connected)
- 2014 Air Force Association’s CyberPatriot Order of Merit
- 2013 GTRA’s GOVTek Executive Gov’t Technology Award for *Excellence in Education*
- Director of National Counterintelligence Executive (NCIX) Exceptional Performance Award—2011
- Two time—USAF-level award winner—2001 Lemay Award (#1 bomber crew in USAF) & 2009 Outstanding USAF Computer Network & Information Operations Team (#1 IO Team in USAF)

- Two Time—Assoc of Old Crows National Gold Merit Award winner—senior management, security innovation
- Teaching and shaping the young minds of our world & spending time will my family and travelling the world
- Avid college football fan