Rob McGregor, CISSP

2809 Lakehollow Lane • Flower Mound TX 75028
Phone: 214.548.1952 • E-Mail: rtmcgregor@verizon.net

INFORMATION SECURITY VETERAN

Business experienced, well articulated, information security management leader with more than 15 years of metrics based result driven experience in developing, executing, and maintaining long-term enterprise wide protection strategies, with a proven track record of identifying and inoculating operational risks. Strong technical background, product development experience, program management expertise, and exceptional communication skills with a data centric and risk based approach to ensure that business and information security objectives are fully achieved at all levels of the organization. Global experience including direct process management of multicultural environments and personnel, providing unique perspectives to information risk management, information security, privacy, governance and compliance at the people, practice, and process levels.

- Responsible for the creation and maturation of multiple security practices, including process, people and technology, from its infancy, and matured it into a fully capable solution.
- Proven track record of introducing innovation and proactive strategies required to meet the demands of changing global business objectives while increasing information security, protecting privacy and mitigating risks to an acceptable level.
- Ability to liaison, partner with, and gain full cooperation from technical personnel to C-level executives.

EXPERIENCE

VERIZON COMMUNICATIONS, SENIOR MEMBER, 2007 – Present
Verizon Enterprise Computer Incident Response Team - Risk Intelligence Officer (RIO), Threat Intelligence Officer (TIO). Global Security Operations Center (GSOC) Liaison Officer, Computer Incident Response Team Coordination Officer. Enterprise/LOB level primary authority for advice, consultation, and direction concerning risk intelligence and threat intelligence operations. Analyze information security (INFOSEC) vulnerabilities and provide recommendations to improve the security posture of systems, applications, and networks. Determine the impact of emerging systems or methods, assess the relative computing environment, assess the relative risk to information compromise, and advise accordingly. Responsible for the full life cycle of enterprise information application and security assessment services. Consult, plan and conduct security consultations for internal and external accreditation projects. Recommend new revised security measures and countermeasures. Provide technical guidance and advisement to application development teams, technical specialists, engineers, and management in areas such as software development lifecycle, security engineering lifecycle, network communication, systems and application development, and documentation. Oversee and enforce data security standards for protection of information resources, and recommending appropriate security safeguards. Responsible for the identification, assessment, and mitigation of inherent, residual, regulatory, security, and compliance based risks. Draft trend analysis reports concerning possible threats to advise executive management.

BANK OF AMERICA, SENIOR SECURITY ARCHITECT, 2006 - 2007
Father, champion, and create multiple risk mitigation programs. Primary authority for advice and guidance in the areas of security architecture, systems auditing, security tools, and all areas related to INFOSEC. Conduct risk, threat, and vulnerability assessments and mitigation programs. Established and maintained a successful information security compliance program as well as implement risk management in to the business life cycle process. Protect computer network systems by identifying vulnerabilities and potentials for attacks. Discover methods of protecting global networks, computer systems, or specific hardware or software. Design, demonstrate, develop, implement, or update protection methods and recommend mitigation strategies and techniques. Initiate investigations concerning rogue and orphaned systems on the network. SME/SPOC for all Exploit Management Team issues.
Accomplishments: - Conducted gap analysis and inventory of system compliance and implemented cross-functional advisory committee. - Successfully proposed, implemented, and maintained 20+ security risk reduction programs with 100% issue inoculation.

COMPUTER ASSOCIATES, SENIOR SECURITY CONSULTANT, 2003 - 2006
Subject Matter Expert concerning all aspects of network based forensics investigations. Architected and implemented forensic investigation practices. Manage day to day activities for projects involving computer forensics, information security or rapid response data breach matters. Manage large data preservation and collection activities. Create and maintain Chain of Custody and document the handling of evidence. Conduct cross functional multi-tier log analyses and relational ontology overlays. Conduct forensic analysis and write applicable directive reports; affidavits; and documentation of findings. Manage large scale and long term projects. Independently perform standard computer forensics activities to advise senior consultants, consultants and associates. Collect and preserve data using accepted forensic protocols; create and maintain chain of custody; document the handling of evidence. Conduct forensic analysis,

interpret results and construct affidavits and formal reports. Manage projects and mentor other project team members. Present finding to clients both formally and informally.
Accomplishments: - Member and trainer for Rapid Response Investigation Team - Expert knowledge and of use of SILENTRUNNER, former NSA forensics toolkit. Provided guidance to further develop and enhance software solution.

VERISIGN, SECURITY PRACTICE MANAGER, 2000 - 2002
Responsible for the overall strategic direction, growth and management of the Security Assessment, Penetration Testing, and Virus Incident Protection Eradication & Response (VIPER) practices within VeriSign. SME for all areas related to INFOSEC. Develop cradle to grave cross functional vulnerability, threat, and inoculation strategies. Implement various regulatory compliance practices. Consult C level executives concerning all issues of INFOSEC. Develop long term permanent security practices for large scale environments and companies. Educate employees and staff concerning security issues, concerns, and initiatives. Responsible for the full life cycle of enterprise information security assessment services. Provide leadership, guidance and oversight for all team operations. Design and develop the portfolio of related service offerings. Help consultants set and achieve personal goals through mentoring and coaching. Track consultant performance utilization and other Practice metrics to determine Practice health and identify opportunities for improvement. Identify opportunities for operational improvement and lead the development and roll out of new consulting methods and tools. Develop relationships with key partners and organizations. Recruit and perform technical and onsite interviews for new hires.
Accomplishments: - Architected, developed, and implemented multiple regulatory compliance practices to include NIST, SOX, GLBA, HIPAA, PCI, and ISO27001 practices. - Creator and Team Leader for VIPER, a self managed incident/rapid response team dealing with computer intrusions and forensics practices.

EDUCATION

Master of Science, Information Assurance Engineering, Capitol College, Laurel MD. , 2012

SKILLS

Streamline Process Improvement ~ Strategic Plan Development ~ Vulnerability and Threat Management~ Crisis Management ~ Liability Management ~ Risk Management ~ Infrastructure & Operations Security Management ~ Identity & Access Management ~ Secure Development Management ~ Distributed/Centralized ISMS ~ Outsourcing ~ Privacy Incident Response ~ Compliance/Governance ~ Security Architecture ~ Policy & Standards Development ~ Global Execution Security Assessments ~ PCI /SOX/ISO 27001 ~ Project Management ~ Contract Negotiations ~ Budgeting & Planning Security Strategy ~ Vendor Management ~ Leading/Mentoring/Motivating/Training ~ Critical Problem Solving ~ Critical Decision Making ~ Exceptional Listening Skills

MILITARY SERVICE

UNITED STATES MARINE CORPS, SERGEANT OF MARINES, 1986-1992
Conduct covert surveillance operations. Advise unit commanders concerning clandestine military operations. Analyze and evaluate plans, programs, projects, policies, standards, guidelines, and procedures to develop the basis for institutionalizing and reviewing security concerns and implications. Conduct physical penetration testing of military units and installations in order test combat readiness.
Accomplishments: - Awarded Meritorious Mast for clandestine operation surveillance and recovery of enemy encryption data 1990. Promotions include Private, Lance Corporal, Corporal, and Sergeant.