RAINMAKER
CONSULTING RESOURCES

Keith Taylor

kmtaylortx@gmail.com | **832-540-1095**

SUMMARY

Cybersecurity Professional with 12+ years of hands-on technology experience in Enterprise Information Security Consultancy, protecting client's infrastructure, corporate data, and customer assets, and ensuring alignment with applicable regulations and laws. Leading cybersecurity risk assessments that addresses policy, process, operations, people, and technology,

Key competencies:

Enterprise IoT
Data Protection & Privacy
3rd Party Security Management
System Configuration / Hardening
Cloud Architecture (AWS/ Azure)
Identity & Access Management
Physical &Environment Security
Information Asset Management
Network Security Configuration
Incident Management
IS Policy & Compliances
Business Continuity / DR

PROFESSIONAL EXPERIENCE

Tg3 Information Security Group - Northeastern Region **09/ 2016 – Present**
Senior Manager, Enterprise Information Security Risk- Consultant

Responsible for creating strategy, policy, meeting regulatory compliance, risk assessments, identification and mitigation, security architecture and standards for our financial clients.

- Acts as a technical consultant for the enterprise, ensuring security design for systems align with business needs, architecture and technical standards.
- Leading and Conducting assessments of third/fourth party vendors. Documenting assessment results and writing assessment reports for key stakeholders in conjunction with, (e.g., ISO 27001/2, COBIT, SOX, HIPPA, FFIEC, HITECH, CSF, SOC2, NIST 800-53) and/or Enterprise Risk Management frameworks (e.g., COSO ERM, ISO 31000).
- Build strong relationships and collaborate with external /3rd party customers and internal technical, business, credit risk, market risk legal partners.
- Implementing OneTrust privacy management software to perform risk assessments, security domain risk assessments, executing data mapping and inventory of critical components of client privacy program.
- Facilitate end-to-end risk management and tactical processing of risk and remediation plans using existing tools such as OneTrust, RSA Archer and Open Pages
- Conducted client workshops on can help achieve General Data Protection Regulation (GDPR) compliance Articles 6,30,32
- Communicate authoring risk assessment reports; particularly for information security programs including Cloud and Virtualized environments to stakeholder's findings from risk analyses, as well as data required to perform risk mitigations.

- Proactively reviews and analyzes new or proposed security systems, tools and methodologies, assessing their risk and their value in support of security strategy and corporate goals.

Deloitte & Touché **01/ 2016 - 08/ 2016**
Advisory Manager- Cyber Risk Services- Consultant

Responsible for advising clients (Financial, Life Science, Manufacturing), with developing technical requirements, evaluating vendor solutions, developing architecture & design, and testing of data protection and data security solutions

- Reviewed technology and security projects, making recommendations with regard to product selection, configuration and design.
- Designed and overseen the implementation of security networking components at the internal and external network perimeter including technologies such as IDS/IPS, Next Generation firewalls, Port Authentication (using CISCO ISE), Web filtering technologies as well as deep packet inspection devices.
- Led implementation with enterprise security solutions such as Endpoint Protection (DLP/Whitelisting/HIPS), WAF, IPS, Anti-DDOS, and SIEM.
- Built security reference architecture for on premise, all-in cloud deployments, and hybrid scenarios
- Conducted security assessment, working in vulnerability management and collaborating with SOC in the investigation of cyber security events.
- Led implementations of the entire ecosystem of data protection architecture implementation of OneTrust DLP, PKI, and Encryption, tokenization, masking and redaction

CGI **01/ 2014 - 11 / 2015**
Partner Director, Consulting Services –Cybersecurity ICS

Responsible for conduct readiness assessments and develop tailored remediation plans to help Financial clients move towards compliance within **General Data Protection Regulation**(GDPR).

- Frequently partnered with internal and/or third-party privacy and project management stakeholders to provide counsel throughout the life cycle of GDPR compliance programs.
- Embedding GDPR Article 30,32, and 6 principles and advising on regulatory best practices in relation to organizations handling of personal information.
- Designing and implementing legal and technical enterprise privacy-governance structures to manage international data transfers (both intragroup transfers and third-party transfers), including EU-US Privacy Shield, EU model contract clauses, and binding corporate rules (BCR).
- Worked collaboratively with clients C-level executive and key business units leads, and 3rd party vendors performing current state, target state, and roadmap assessments. remediation, implementation, and integration of governance & risk end-to-end solutions.
- Performed cyber risk assessments and developed response strategies based on current state, developed target state, developed 3- 5-year mitigation roadmap, based on NIST 800-53 and ISO

Tg3 Information Security Group **03/ 2008 – 01/ 2014**
Co-Founder & CISO -Cybersecurity

Start- up, Responsible for leading a team working with a National practice, which often times includes global team members, working with organizations to determine long-term goals, identify opportunities, and analyze action plans for organizations to achieve their overall Cybersecurity objectives.

- Performed cyber risk assessments and developed response strategies based on current state, developed target state, developed 3- 5-year mitigation roadmap, based on NIST 800-53 and ISO 27001/2, HITECH, HIPAA, cybersecurity framework NIST CSF, COBIT, COSO, and PCI standards, minimizing risk and ensuring business continuity by limiting the impact of a security breach.
- Led the General Data Protection Regulation (GDPR) team assessing and implementing security programs or specific capabilities, including governance, incident response, threat intelligence, security monitoring, training, and awareness
- Acted as a subject matter resource in specific programming languages and web application environments. Propose vulnerability risk level and estimated level of remediation effort. Propose code fix or architectural strategies to remediate identified vulnerabilities. Confirm appropriateness of a proposed remediation approach or propose viable alternatives and perform the actual remediation.
- Collaborate with the engagement team to plan the engagement and develop work programs, timelines, and planning documentation. Work with the team to document the business processes dependent on IT. Ensure high-quality client service by directing daily progress of fieldwork, informing supervisors of engagement status, and managing staff performance.
- Assessed and provide guidance on emerging security related guidance as related to the OCC, FDIC and FFIEC, as well as, other regulators within the financial industry.

U.S. Department of Justice –CRS **09/2001 – 02/2008**
Cybersecurity Analyst

Responsible for the development, implementation and management of complex Enterprise Cyber Security-Information Systems Security Programs, Information Assurance Risk Management Programs and Insider Threat Programs for the; DoD, National Level Intelligence Centers, Defense Industrial Base Contractors, U.S Government Agencies, State Governments, large and small businesses.

- From the ground up, I developed, implemented and managed an Enterprise Top Secret SCI Cyber Security-Information Systems Security Program for the Defense Intelligence Agency-National Media Exploitation Center.
- Protected the confidentiality, integrity and availability of mission critical classified-unclassified information and information systems.
- Applied defense-in-depth strategies using multiple layers of security; Physical / Operational Security, Network Perimeter, Application Layer, Storage Layer, Data Layer, End Points.

IT Manager **07/1991 - 09/2001**

- Major Responsibilities Have Included: Security Policy and Security Classification Guide Development, Data Privacy Protection / Personally Identifiable Information (PII), Conducting Risk Assessments / Mitigation Guidance, Performing Certification / Accreditation of Classified / Unclassified Information Systems.

EDUCATION

Bachelor of Science in Computer Science Southeastern University

CERTIFICATION

Certified Information Systems Security Professional – CISSP