Mary N. Chaney, Esq., CISSP

4501 Georgiana Lane
Mansfield, TX 76063
(682) 518-3160 (home)
(682) 412-0084 (cell)
Email: mary@mnchaneylaw.com
Web: https://vimeo.com/78118455

I am a licensed attorney with significant operational experience in cyber security, privacy and risk management. I have lead teams responsible for cyber-incident management, incident response, cyber-network defense, forensics and e-discovery, internal threat, database security management, security awareness, and data leak prevention, to name a few.

During my career I have also developed and performed risk assessments, business impact analyses, incident response plans, business continuity and disaster discovery plans, drafted information security policies and procedures for small, medium and large enterprises. If it is related to cyber security, I have done it!

~ CISSP, Certified Information Systems Security Professional, 2008 ~

AREAS OF EXPERTISE

Drafting Information Security Policies and Procedures │ Information Security and Information Risk Assessments and Audits │ CISSP | Information Security Awareness Training │ Security Incident Response and Investigation │ Legal and Regulatory Compliance │ Privacy and Data Protection │ Asset Management │ Business Continuity Planning │ Disaster Recovery Planning │ SOX | HIPPA | GLBA| FFIEC | Human Resources Security │ Physical and Facility Security │ IT Contract Drafting and Auditing | Leadership

PROFESSIONAL EXPERIENCE

The Law Offices of Mary N. Chaney, P.L.L.C. 01/2018-Present

- The goal of the Law Offices of Mary N. Chaney, P.L.L.C is to help translate and advise, Boards of Directors, CIO's, CISO's and General Counsel's on how to legally protect their company from cyber related risk.

- Our services include overall cyber security program review and assessment, cyber contract negotiation and review, 3rd Party vendor compliance review and assessments, drafting cyber related policies and procedures, internal regulatory compliance assessments, business impact assessments, security incident response and many privacy related matters. So, if you are looking for an attorney that knows the ins and outs of cyber security, that can speak geek as well as legalese, The Law Offices of Mary N. Chaney, P.L.L.C. is the firm for you!

International Consortium of Minority Cybersecurity Professionals 06/2017-Present
Vice President

- ICMCP’s mission is to build a pipeline of diverse cybersecurity talent that will ensure underserved populations reach the level of cybersecurity education and proficiency they choose to pursue by creating cybersecurity opportunities from Pre-K throughout their entire working career.

- Through various programs we assist with promoting public awareness of cyber security and the opportunities for women and minorities in the profession.

- We work to increase the number of women and minority students pursuing cybersecurity related disciplines at both the undergraduate and post-graduate levels by funding scholarships opportunities.

- We facilitate the career advancement of existing member cybersecurity practitioners through mentoring, grants towards advanced degrees and professional certifications in the field of cyber security.

- We function as a representative body on issues and developments that affect the careers of women and minority cybersecurity professionals.

MBS Information Security Consulting, LLC, Cincinnati, Ohio
Founder & CEO ***08/2008 – Present***

- MBS provides information security consulting, training, and outsourcing services for small and midsized businesses. We specialize in the delivery of sensible and affordable information security solutions for our clients, based on their business mission.

- MBS creates Information Security Management Programs for our clients around their business. This includes creating, drafting and publishing all necessary policies, procedures, manuals, response plans, business impact analysis, BR/DR plans, and training. The programs were designed to effectively establish, implement, monitor and improve controls to ensure that the security and business objectives of an organization come together.

Comcast Corporation, Philadelphia, PA
Senior Director, Information Security ***08/2016- 05/2017***

Member of the Global CISO's (GCISO) office which has oversight responsibilities for both Comcast Cable and NBC Universal for Cyber Risk Management. In this role, my responsibilities include reviewing, assessing, and developing strategy to ensure information securities policies, procedures, and standards are applied effectively across the Corporation. In addition, developing a cyber risk metrics dashboard that shows the Corporations cyber risk posture across a multitude of areas.

- **Tools Governance** - Collaborated across the business units to build an inventory of 171 security tools. Collected financial and contract data to analyze historic and planned spend on identified security tools. Identified how and where the organizations spend on security technologies based on spend analysis and security tool capability mapping. Designed a security tools governance framework that defines how the GCISO organization will interact with the security teams to guide future investments in security tools.

- **Third Party Assessments** – Assisted with the development of a questionnaire that was designed to assess the potential "loss of data" risk to the overall corporation of various 3rd parties. Interviewed 3rd parties that self-identified "high" data risk to determine if risk reached the appropriate threshold for the definition of high data risk to the Corporation.

- **Data Governance** - Performed scans of unstructured data in file shares, i.e. data in word docs, excel spreadsheets, etc. to assist the businesses with identification of where sensitive data may be stored in unsecured ways.

- **Brand Awareness** – Developed a model whereby each individual business unit was graded utilizing various internal and external factors including their external brand reputation utilizing Bitsight.

Johnson & Johnson, Raritan, NJ
Director, Worldwide Information Security ***03/2015- 8/2016***

Led a Global team of eighteen (18) employees and (15) contractors that form a blended 24x7 Security Operations Center (SOC). Responsibilities included restructuring SOC to align with the Kill Chain©

methodology and developing and implementing the required mission, vision, goals, strategic direction and operational functions to align with that methodology.

Program Highlights:

- Completed full restructuring and aligned program responsibilities to the Kill Chain© methodology.

- Streamlined SOC tools and technologies which resulted in a reduction of approximately 200k per year in operating budget.

- Activated additional security functionality on currently deployed technologies to provide increased control over end-points which resulted in increased visibility and a reduction of containment times.

Program Structure and Responsibilities:

- **Intelligence & Investigations** – Program responsibilities include cyber-intelligence creation, fusion, collection and analysis, distribution of J&J relevant intelligence to internal business and IT stakeholders, trending, and conducting threat assessments. In addition, insider threat investigations, lost and stolen devices, and litigation case support.

- **Threat Prevention** – Program responsibilities include border protection device operations and maintenance, sensor tuning and maintenance, custom signature creation, tool research and development, global web categorization policy management, external partner connection analysis, client/server policy management.

- **Threat Detection** – Program responsibilities included management of our manage service provider L1 resources which includes call center, real-time monitoring and initial triage. The internal J&J team is responsible for escalated security alert review (L2/3). In addition, driving for enterprise log standardization, ensuring appropriate log data is collected and distributed, log content creation and management for our security event management environment.

- **Cyber Incident Management** – Program responsibilities include cyber-incident response and investigation, incident root cause analysis, tradecraft analysis, countermeasure implementation, forensic artifact handling, malware reverse engineering, and forensic artifact collection and analysis.

GE Capital Corporation, Cincinnati, Ohio
Senior Team Leader – Information Security ***04/2012 – 03/2015***

Led a team of (4-6) employees who were involved with a multitude of information security responsibilities that supported over 14,000 GE Capital America (GECA) end-users. Responsible for creating, drafting and publishing IT security policies, standards and procedures to support the overall mission of several key areas including:

- **Incident Response** – Monitoring, detecting, alerting and responding to security concerns in the GECA environment. This includes lost and stolen devices, malware infections, denial of service attacks, internal misuse, etc. In addition, running relevant exercises that test the coordination of stakeholders in the event of an incident.

- **Forensics/E-Discovery** – Oversees forensics and e-discovery investigations to ensure timely completion. Responsibilities include validating, forensically imaging and documenting any internal or external subpoena request.

- **Database Security Management** – Oversee security related changes to our computer databases. Also plans, coordinates, and implements security measures to safeguard computer databases and secures the flow of data with various tools at the ingress and egress points.

- **Security Awareness** – Developed the overall security awareness program for GECA. Responsibilities included the establishment, coordination and oversight of training for end-users, IT users with highly privileged access, and application developers. This includes running employee phishing exercises and working with outside vendors for relevant training.

- **Data Leak Prevention** - Establishes the rules and policies related to data leak prevention program. Leads the exception process related to the use of removable media in GECA and monitors and responds to any security concerns regarding the movement of data.

University of Cincinnati, Cincinnati, Ohio
Adjunct Professor ***01/2012 – 01/2015***

Courses:

- **Information Security & Assurance** – This course was an introduction to the various technical and administrative aspects of Information Security and Assurance. It provides the foundation for understanding the key issues associated with protecting information assets, determining the levels of protection and response to security incidents, and designing a consistent, reasonable information security system, with appropriate intrusion detection and reporting features.

- **Network Security** - This course covers an array of technologies (firewalls, IDS, VPN) and techniques (defense in depth, ACLs, host hardening) to secure a computer network. Students learned to anticipate network weaknesses through penetration testing and design of the network infrastructure and policies to preempt potential attacks upon the network.

- **Enterprise Network Administration** – This course covers advanced current topics in network/system administration. It provides a survey of technologies used within the technical enterprise for efficiency and stability of the network.

- **Routing and Switching** – This course covered construction of network segments and linking those segments together with routers and switches. Once networks were connected, issues such as network interoperability, real-time network analysis, and Quality of Service (QoS) were addressed. Students also learned topics about router programming and built applications for the router.

Federal Bureau of Investigation, Los Angeles, California
Special Agent, Information Systems Security Officer,
Associate Chief Security Officer ***06/2002- 06/2008***

- **Special Agent** – Federal cyber-crime investigator, cases involved computer intrusion, intellectual property theft, copyright infringement, internet piracy and other cyber-related fraud activities. Familiar with forensic tools used in connection with case investigation and review.

- **Information Systems Security Officer /Associate Chief Security Officer** – Responsible for the overall development and oversight of the Information Security and Privacy program for the Los Angles field office. Responsibilities included approving security clearances and 3rd party access, systems and service acquisitions, physical security, systems maintenance, incident response, certification and accreditation, risk assessments, business continuity and disaster recovery, and awareness and training. In addition, made relevant changes in the environment that were site specific and documented those changes for auditor review.

EDUCATION / CERTIFICATIONS AND LICENSES / AFFILIATIONS

EDUCATION:

- Thurgood Marshall School of Law, Texas Southern University, Houston, Texas, 1999

Juris Doctorate, ***Summa cum laude, Salutatorian***

- Xavier University, Cincinnati, Ohio, 1994
  Bachelor of Science in Business Administration, Information Systems

CERTIFICATIONS & LICENSES:

- C.I.S.S.P. ID# 319200, State Bar of Texas

CLEARANCES:

- Secret