

Cyber Legal & Security Litigation Support

Overview

The legal arena has always been characterized by new developments and change, and cyber security law is no exception. Whereas two decades ago cyber security law had little impact on organizations' plans, actions and strategies, the opposite is now very much true. Legal actions are in particular commonly connected to information technology issues and electronic data leakage. For example, a lawsuit requiring thousands of hours of effort could result after a competitor deliberately attempts cyber espionage on an organization's information processing systems. Emagined Security's Cyber Legal & Security Litigation Support practice provides a variety of services related to cyber security legislation and its impact, how to conduct investigations, expert advice and testimony and much more.

Benefits

Legal action on both the plaintiff and defendants side can have a dramatic impact on an organization's business initiatives. Without the proper support, legal actions can cripple an organization's ability to conduct business. Whether initiated by a disgruntled employee, a malicious competitor or a business partner, legal actions often cause damage and disruption equal to or greater than any natural disaster.

Emagined Security's specialists can provide a variety of litigation support services efficiently, expeditiously and confidentially. For example, litigation support response team can be deployed to perform remote and on-site legal action management, develop and validate action plans, and support investigations while minimizing the impact on business operations.

Description of Service

Emagined Security can deploy a litigation support response team to support Cyber Legal & Security Legal Action. Our services include the following:

- Legal Action Preparation
 - Legal Action Response Planning
 - Legal Action Response Plan Development
 - Legal Action Response Plan Validation and Assessment

- Legal Action Response
 - Legal Action Management
 - 24x7x365 On-Site Response
 - 24x7x365 Remote Response
- Legal Action Analysis
 - Data Capture
 - Research on statutes and rulings
 - Digital Forensics
 - Deposition Acquisition & Analysis
- Litigation Support
 - Evidence Discovery
 - Expert Witness Selection and Advice
 - Expert Witness Testimony
 - Cyber Legal Services
 - Evidence Custodianship
- Compliance and Regulation Support
 - Familiarization with and interpretation of compliance requirements
 - Compliance and regulation controls and procedures
 - Assessment of compliance and regulation measures
- Training in Cyber Security Legal Issues
 - Course on cyber security legal issues
 - Short training sessions with a focus on specific issues

Throughout these services, Emagined Security can assist in collecting and handling data to be used as evidence. Upon request, we can deploy a team of highly trained and experienced Incident Response and Cyber Forensics experts. Our team can perform research, provide detailed reports and serve as expert witnesses. Additionally, our staff can proactively work with your organization to provide ongoing assistance and recommendations to preclude the need for future legal actions.

Emagined Security Personnel Qualifications Include

- Testimony on proposed cyber security legislation before U.S. House and Senate Subcommittees
- Expert witness testimony in various civil cases
- Experience as cyber security liaison to Berkeley Lab legal department
- Consulting for law firms (including research on cyber-security-related court rulings and patent infringement claims)

- Co-developed National Institute of Standards and Technology (NIST) Guideline for Incident Response (2001)
- Authorship of book chapters on cyber security issues including “Incident Response – A Strategic Guide to Handling System and Network Security Breaches”
- Certified Information Systems Security Professional (CISSP) certification
- Certified Information Security Manager (CISM) certification
- Membership on Accreditation Board for Institute of Information Security Professionals (IISP)

Emagined Cyber Security Litigation Experts

Dr. Eugene Schultz, Chief Technology Officer and Executive Consultant

Dr. Schultz has received the NASA Technical Excellence Award and the Information Systems Security Association (ISSA) Professional Achievement and Honor Roll Awards, and has been elected to the ISSA Hall of Fame. While at Lawrence Livermore National Laboratory, he was the founder and original project manager of the U.S. Department of Energy's Computer Incident Advisory Capability (CIAC) and also a co-founder of FIRST, the Forum of Incident Response and Security Teams. He has provided expert testimony before committees within the U.S. Senate and House of Representatives on various security-related issues, and has served as an expert witness in legal cases.

Earl Cunningham, Security Director and Executive Consultant

Mr. Earl Cunningham is an experienced senior level Information Security professional with 30+ years of demonstrated expertise in information security governance and management. He established and managed enterprise-wide global information security incident response program for Visa, Inc. He is NSA certified and trained as a Russian linguist intelligence specialist. During these efforts, he conducted communications and signals intelligence collection operations against Soviet block military and government entities worldwide.

James G. Robinson “Gary”, Executive Consultant

Mr. Gary Robinson was the Lead Information Security Member of Visa's Command Management Team for the Global Emergency Operations Center, and established Visa's Compliance Monitoring, Content Analysis, Incident Response, Forensic & Application Penetration programs. He has combined extensive law enforcement experience to establish, direct and lead a team of computer security professionals in the analysis and recommendation of appropriate computer and communication security protective measures to address fraud, waste, and abuse of resources and classified national security measures. He has managed Federal, State, and Local computer security incidents, and monitored the Visa networks for intrusion, fraud, waste, and abuse.