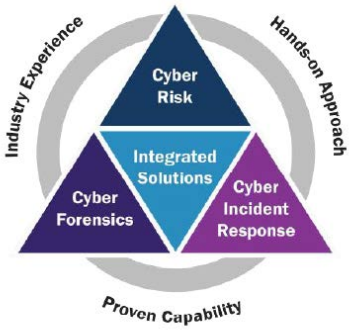
GLOBAL INSURANCE SERVICES

Cybersecurity Services

Cybersecurity Services

Clients rely on FTI Consulting to help manage a wide range of forensic issues in the increasingly complex user and enterprise technology environment including:

- Cybersecurity resilience check
- Cybersecurity culture assessment
- Cybersecurity awareness training
- Cybersecurity risk assessments
- Cybersecurity incident response
- Cyber Forensics
- Data / Privacy breach investigation
- Information security consulting
- Cybersecurity analytics



The increasing use of technology in the workplace and for delivery of business services, along with the complexity of enterprise information systems, requires a sound forensic technology response to Cybersecurity or data breach incidents.

Good cyber governance should include regular cyber risk management activities including the development of appropriate policies and procedures, risk identification and analysis, and staff and supplier training and awareness.

Whether it is in response to a corporate security incident, information security breach, internal staff misconduct, data from the organization’s IT systems will need to be collected and analyzed in order to find relevant and accurate information regarding the incident or circumstance s of the event and the potential security improvements required to help minimize the impact of similar incidents in the future.

Our Cybersecurity Capability

FTI Consulting is a leading provider of independent cyber and risk management advisory services. Our professionals are leading specialists in assisting clients manage the risk of cyber and fraud related incidents. Our security and risk practitioners are also forensic specialists with a wealth of experience in dealing with technology, fraud and security matters.

Drawing on our extensive experience in law enforcement, system security consulting, and incident response we can provide the highly specialized skills required to investigate Cybersecurity incidents, identify the potential source or cause of the incident and to identify potential security improvements.

FTI Consulting can provide a comprehensive range of cyber risk and security services.

Cyber Forensic Laboratories

Our teams have access to dedicated forensic technology laboratory systems, which include specialized forensic software tools and forensic field kits.

FTI Consulting uses leading industry forensic hardware and software tools that are widely accepted by commercial and law enforcement forensic specialists. These capabilities enable us to provide an efficient and appropriate response, regardless of the scale or complexity of the technology encountered.

FTI Consulting forensic laboratories are equipped with special purpose workstations and equipment for the preservation, extraction and analysis of data collected; and restoration or replication of application systems such as corporate data bases, document management systems, email, and system backup.

Cyber Risk & Security Consulting

In order to assist organizations in improving their understanding of Cybersecurity practices, procedures and controls, and to assess the potential security improvements that may be required, we provide the following cyber risk and security consulting services:

- Cybersecurity Resilience: Health Check
- Cybersecurity Framework Review
- Cybersecurity Risk Assessments
- Cybersecurity Incident Response Planning
- Cybersecurity Maturity Assessment
- Cybersecurity Culture Assessments / Training

Adapted specifically for each client, our Cybersecurity Culture Survey is designed to gain an understanding of the organization's culture and its capacity to prevent, detect and respond to Cybersecurity incidents. It will also provide insight into staff perception of cyber risks and their awareness of the organization's Cybersecurity controls.

Based on the findings of our Cybersecurity Culture Survey we are able to develop Cybersecurity Staff Awareness Training to educate staff regarding current and emerging Cybersecurity threats and the organization's expectations of staff to recognize and appropriately respond to cyber risks or incidents.

Cyber Forensic Analysis

Our Cyber forensic team assists clients to identify data sources required to be preserved regarding a security incident. We use forensically sound techniques to collect potential electronic evidence from a wide range of sources, such as user systems and devices, corporate email, web, financial, application, security and other network devices, in order to undertake the following advanced investigative analysis

- Email or chat tracing and analysis
- End user and corporate system activity analysis
- Internet and web based system activity analysis
- System and network monitoring and logging
- User online & social media activity analysis

Cyber Data Breach /Privacy Incidents - Cybersecurity Incident Response

In order to determine the source and nature of technology or Cybersecurity incidents, a sound forensic investigation response is required. Drawing on our extensive experience in law enforcement, system security consulting, digital forensics and computer incident response, we can provide highly specialized skills required to respond, investigate and recover from cyber incidents including:

- Confidential information disclosure ("leaks")
- Intellectual property ("IP") breaches
- Employee system misuse
- Online or computer fraud
- Cybersecurity incidents
- Network or system intrusions
- Data breaches / privacy incidents
- Critical system or other technology incidents

Based on the investigation work undertaken, we provide reports of our investigation findings, recommendations regarding potential security improvements identified or expert forensic reports and expert technology evidence for legal proceedings.

Cybersecurity Analytics

Our Cyber forensic team assists clients to proactively undertake the following types of advanced forensic analysis to gain insight into potential previous suspicious activity that may be indicative of a security breach or future Cybersecurity threats requiring a security or investigation response.

- Suspicious system or network activity analysis
- Security incident and compromise analysis
- Cyber fraud & anomalous user behavior testing
- System logging and monitoring assessment

Potentially suspicious or anomalous system or user activity identified can then be further forensically analyzed to assess or investigate an incident to determine the nature or source of the attack.

Paul Braithwaite
+1 212-499-3659
Paul.Braithwaite@fticonsulting.com

Wendy Shapss
+1 212-841-9374
Wendy.Shapss@fticonsulting.com

Jim Wrynn
+1 212-841-9366
Jim.Wrynn@fticonsulting.com

FTI™ CONSULTING

About FTI Consulting

FTI Consulting, Inc. is an independent global business advisory firm, dedicated to helping organizations manage change and mitigate risk: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. Connect with us on Twitter (@FTIConsulting), Facebook and LinkedIn.

www.fticonsulting.com