SERVICE SHEET

Cybersecurity Energy Capabilities

An intelligence-led, expert-driven, strategic approach to global cybersecurity challenges affecting your organization – your people, your operations, and your reputation.

The global energy sector is increasingly interconnected, automated, and digitized than ever before — with expanded deployments of advanced technology solutions such as smart grids, smart meters, smart cities, and digital oilfields. While technological advances have led to improved efficiency, they have also increased the energy sector's exposure to cyber threats.

Cyber Risks Facing the Energy Sector

- Interconnectivity
- Legacy equipment
- Persistent threats
- Supply chain
- Mobile devices
- IT/OT system penetration
- Ransomware
- Denial of Service

Industry Outcomes from a Cyber Attack

Clean Energy

- Negative physical impacts to local environment and community
- Effects of attack are capable of quickly spreading to other entities

Oil and Gas

- Competing nations gain political and economic leverage
- Inability to manufacture/deliver product

Chemicals

- Loss of production
- Intellectual property theft

Power & Utilities

- Power outages could severely impact financial, communications, transportation, & water networks
- Destruction/theft of customer data

HOW FTI CYBERSECURITY CAN HELP ENERGY COMPANIES

- Perform cybersecurity program assessments to ensure proper protections are implemented
- Conduct policies, procedures, and staff gap analysis and design
- Assist with federal regulation cybersecurity compliance readiness
- Develop and test incident preparedness and response plans
- Execute crisis simulation and table-top exercises
- Provide crisis management and strategic communications support after a breach

Cyber Readiness

All organizations are vulnerable to cybersecurity risk. Building a robust security posture is the best way to prevent a breach from occurring. Effective and tailored incident prevention measures can help preserve your corporate reputation, operations, and financial standing.

- Cybersecurity Program Assessment
- Penetration Testing
- Threat-hunting Operations
- Policies, Procedures, Staff Gap Analysis & Design
- Vulnerability Assessments
- Red Teaming
- Cybersecurity Compliance
- Information Governance, Privacy & Security
- Dark Web Intelligence & Monitoring
- M&A Due Diligence
- Third Party Assessments
- Crisis Simulation & Table-top Exercises

NERC-CIP Compliance Standards

FERC Order No. 848 and CIP 013-1, CIP 010-3,CIP 005-6

- Evaluation of vendor cybersecurity practices and procurement risk determination
- Vendor disclosure of known vulnerabilities
- Verification of software source code and updates/ patches
- Technical ability to authorize, monitor, control, and disconnect sessions for human interactive and machine-to-machine sessions

FERC Order No. 848 and CIP 00806

- Mandatory reporting for cybersecurity incidents that compromise, or attempt to compromise
- Detailed cybersecurity incident response plans and key supporting details for plan implementation
- Implementation plans must be tested and maintained

Critical Asset Telemetry & Data Automation for a Multi-Billion Dollar Energy Company

A multi-billion dollar energy company needed assistance in organizing their critical asset telemetry to more effectively identify, quantify, and mitigate cyber threats in real time. FTI Consulting was hired to fully enumerate the critical asset data points, develop custom automation capabilities with centralized data warehousing within the company, and build an application to present varying data views of the real-time threat using NIST standards as a baseline of measurement for assessing risk.

FTI Consulting developed a solution that automates aggregation of current cybersecurity asset telemetry, while building additional collection processes for data currently not capable of automation. The application provides risk and threat information at consumption levels appropriate for C-Suite strategic consideration to line level tactical supervisory utilization in mitigating threats across the enterprise.

Program Development & Supply Chain Risk Management

In response to the new and expanded standards approved by the FERC, we were hired by a multi-billion dollar energy company to develop an innovative cybersecurity program designed to meet the NERC-CIP requirements prior to the July 2020 implementation deadline.

FTI Cybersecurity is currently developing an automated threat assessment program and a supply chain risk management compliance program. These programs will enhance enterprise awareness of emerging cyber threats and establish and maintain compliance with NERC-CIP standards.

Phishing Emails at a Petrochemical Company

A leading international petrochemical company recently experienced a business email compromise (BEC), a form of highly impactful phishing attack, in which a company employee's communications are imitated with the objective of socially engineering other members of staff into processing fraudulent wire transfers. Unfortunately, three wire transfer payments, totaling $10 million, were made to a bank in Hong Kong and processed by the company's financial director in response to payment instructions he received from several spear phishing emails disguised to appear as if they came from the company's chief financial officer.

The FTI Cybersecurity team conducted an independent cybersecurity investigation with a focus on addressing potential insider threats and determining whether the attacker gained unauthorized access to the client's network and/or email accounts.

Assessment for an Energy Sector Business

In connection with an unrelated internal investigation at a multibillion-dollar energy sector business, our experts identified several cyber vulnerabilities at the company, as well as employees engaged in suspicious activity.

Our team prepared and presented a cybersecurity assessment and a remediation plan to the company's CEO and Board of Directors. In addition, after designing and implementing a cost-effective monitoring program, we identified two employees who were actively stealing trade secrets. The information developed by our investigation led to successful motions for injunctive relief and to the recovery of the stolen proprietary information. We also coordinated successful referrals to federal law enforcement.

Incident Response

All organizations face cyber threats that compromise data and interrupt operations. Once an incident is detected, immediate action is critical. Our experts know how to respond to all threat types and understand that cyber incident response capabilities must seamlessly integrate across existing mission-critical functions.

— Preparation

— Detection & Analysis

— Containment, Eradication & Recovery

— E-discovery

— Data Identification & Review

— In-bound Call Center & Notifications

— Crisis Management & Strategic Communications

Complex Investigations & Litigation

Our team routinely tackles global, large-scale, and complex issues, that often stem from data privacy related concerns, and demand intricate solutions. We quickly unearth key facts and data sets to enable timely and strategic decisions in investigations, leading to cutting-edge and data-driven results.

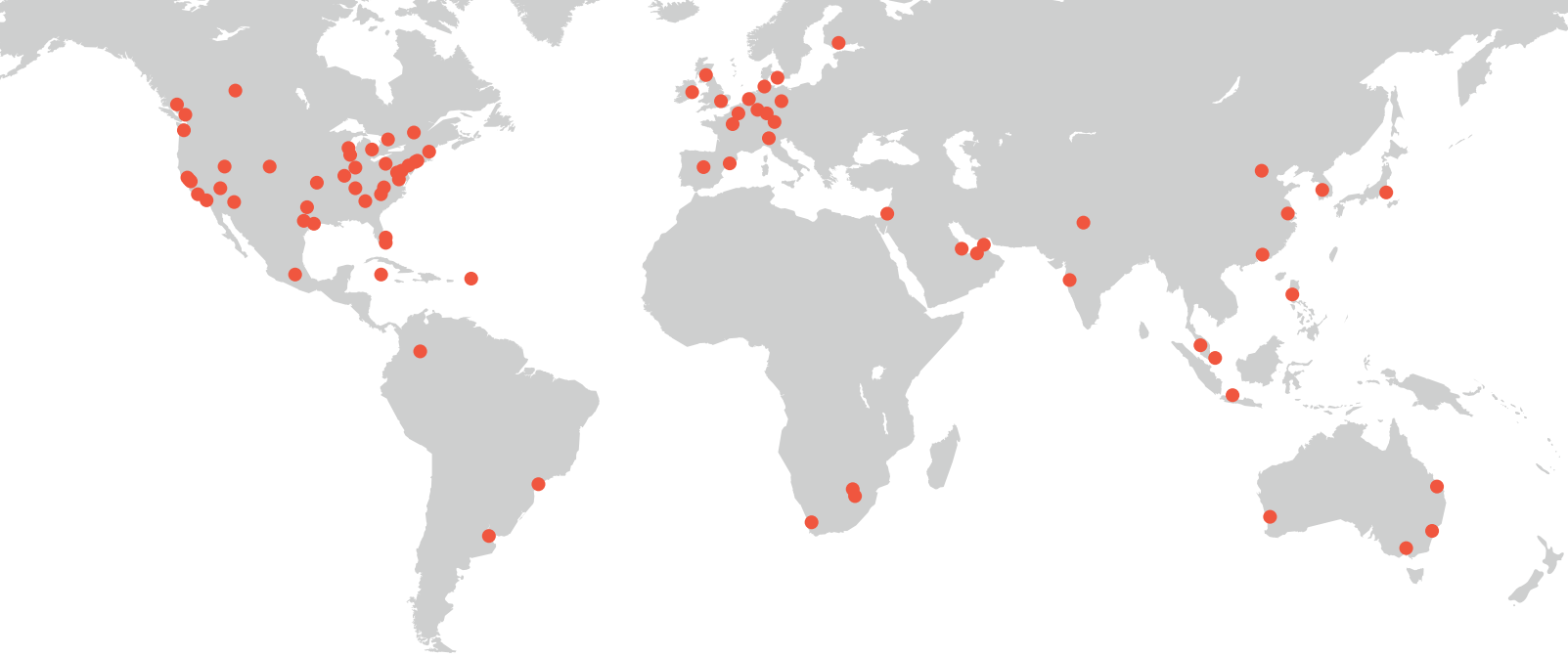
— Litigation Support

— Expert Witness Testimony

— Evidence Collection, Handling, & Preservation

— Forensic Analysis & Complex Modeling

— Data Breach Class Action



Why FTI Cybersecurity

Multidisciplinary Expertise

Intelligence-led, expert-driven, strategic approach to cybersecurity challenges

Core team from intelligence agencies, law enforcement, prosecuting offices, and global private sector institutions

Globally Positioned

Ability to respond anywhere in the world

Ability to staff the largest and most complex engagements and investigations

Relationships with the top global intelligence agencies, regulatory authorities, and private agencies

Integrated & Comprehensive

No other firm in the space has a crisis communications practice

Integration of FTI Consulting's expertise across the platform

1982

Year Founded and $4.9B equity market capitalization*

9/10

Advisor to 9 of the world's top 10 bank holding companies

7,500+

Employees

NYSE:FCN

Publicly traded

98/100

Advisor to 98 of the world's top 100 law firms

59

59 of Fortune Global 100 corporations are clients

**Number of total shares outstanding as of October 20, 2022, by the closing price per share on October 27, 2022.*

ANTHONY J. FERRANTE
Global Head of Cybersecurity
Senior Managing Director
+1 202 312 9165
ajf@fticonsulting.com

JORDAN RAE KELLY
Head of Cybersecurity, Americas
Senior Managing Director
+1 202 312 9140
jordan.kelly@fticonsulting.com

DAVID DUNN
Head of Cybersecurity, EMEA & APAC
Senior Managing Director
+44 7816 251410
david.dunn@fticonsulting.com

01272023 | FTI Cyberse