SERVICE SHEET

Cybersecurity Critical Infrastructure Preparedness & Incident Response

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

Critical infrastructure is more than operational systems and physical assets. It is a complex ecosystem of digital and physical nodes working in concert to seamlessly deliver goods and services that are vital to our daily life.

Due to the complexity and interdependencies of hyperconnected digital and physical assets in critical infrastructure, the required coordination to mitigate risk and respond to incidents is a massive undertaking. FTI Cybersecurity understands the planning required to conduct day-to-day business operations, while simultaneously preparing and training for a critical infrastructure incident.

Our team has extensive experience in industrial systems, facilities, and operational processes with deep industry expertise derived from their backgrounds in government, military, and the private sector. We have a proven track record of harmonizing the technical, operational, legal, regulatory, reputational, and workforce components into workable solutions.

Critical Infrastructure Preparedness

FTI Cybersecurity provides tailored critical infrastructure preparedness policies and programs specific to an organization's industry requirements and customized for stakeholders, ranging from the Board and C-suite to operational managers. Our services include:

- Infrastructure system review and vulnerability assessments
- Policies, procedures, and staff gap analysis and design
- Federal regulation cybersecurity compliance
- Incident preparedness and response planning
- Crisis simulation and table-top exercises
- Workforce development and future personnel/key skills roadmapping

Industrial Incident Response

Should an incident occur, the organizational response is critical to effectively manage the initial incident and ongoing ramifications.

FTI Cybersecurity has a successful track record of providing organizations with:

- Incident containment, eradication, and recovery
- Restoration of operations
- Strategic and crisis communications
- Government regulatory notification
- Government and law enforcement coordination
- Litigation support, including damage quantification, expert testimony, and digital forensic analysis

Critical Asset Telemetry & Data Automation for a Major Energy Company

SITUATION

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. The company's existing program collected numerous data points of significant value as part of their existing cybersecurity program. However, the program required an automated solution to aggregate all available data into a central repository for measurement against National Institute of Standards and Technology (NIST) standards to effectively identify real-time risks across the enterprise.

OUR ROLE

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. We developed a custom application that aggregates various data points and applied a proprietary risk algorithm. The output was a dashboard that displays cyber risk, filterable to allow for both an overall snapshot of the energy company's risk, or as granular as needed based on the job function of the individual viewing the dashboard. This helped display which areas required further attention.

OUR IMPACT

The solution developed automates aggregation of current cybersecurity asset telemetry while building additional collection processes for data currently not capable of automation. The application built to display correlated asset metrics 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.

Large-scale Data Breach Investigation for a Leading U.S. Health System

SITUATION

A leading U.S. health system suffered a large-scale data breach. While the initial attack was limited to food and beverage point of sales systems, the cyber criminals were able to expand their attack deeper into the client's network, gaining access to the personally identifiable information (PII) of over 3 million patients. As a result, a class action lawsuit was brought against the client for inadequate protection of the plaintiff's data.

OUR ROLE

Our team provided data breach response and investigative services due to our interdisciplinary approach to the collection of information housed on the dark web as well as our ability to paint a broader picture of the information that is currently available and correlate the data to show intersections and patterns.

OUR IMPACT

Our dark web information was leveraged to determine if the named plaintiffs were impacted by unrelated data breaches and the extent of information included in those breaches. Our analysis enabled counsel to discount the plaintiff claims.

To find out more about how our services and solutions can help your business, please contact us or visit us at **www.fticybersecurity.com**

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