Insider Threat & Workplace Misconduct

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

Network users with trusted access can exploit the systems that protect your most critical assets, exposing your organization to long-lasting, even permanent, effects on your organizational reputation, intellectual property, and economic security. It is critical for firms to implement policies, procedures, and technologies that address the organizational, behavioral, and technical issues surrounding insider threats.

A comprehensive insider threat mitigation program requires coordinated efforts across stakeholders and addressing risk at all stages.

Prevent: Proper defensive controls can work to prevent malicious insider activity at the outset. FTI Consulting can establish a program that implements a variety of technologies and controls to protect your critical assets, to include security policies, employee awareness training, and access and privilege settings that minimize unnecessary risk to your organization. These controls will allow you to anticipate and manage potential impacts before they impose negative consequences.

Detect: Identifying suspicious and anomalous user activity is a key component of a cutting-edge insider threat program. Critical aspects of this program must include event logging and review, integrity checks, and independent audits of network activity. FTI Consulting can implement a holistic program, based in an understanding of your corporate network governance that will ensure seamless overlay between your daily operations and threat detection.

Respond: In the aftermath of an incident, your organization must move quickly to respond in order to minimize damage. FTI Consulting can immediately implement a response process that includes recovery of processes and assets, forensic examination, necessary quarantining, and credential removal.

Our experts also have extensive experience with workplace misconduct investigations, which may be appropriate in the aftermath of an impact to your networks.

Workplace Misconduct Investigations: Digital misconduct can encompass more than just insider threats. Effective workplace technology investigations require not only extensive experience in network forensics; these investigations must also consider long-term adjustments to policy and necessary actions against the employee, to include litigation. Our experts have the technical capability to undertake the most sensitive investigations, to include conducting discreet forensic reviews through remote cloud-based platforms, while ensuring that your organization minimizes liability and retains its ability to take appropriate action.

Why FTI Cybersecurity

Multidisciplinary Expertise

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

Core team from intelligence agencies, law enforcement, 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

CASE STUDY

Insider Investigation at a Petrochemical Company

SITUATION

A leading international petrochemical company experienced a business email compromise (BEC). Three wire transfer payments, totaling $10M, were made to a bank in Hong Kong and processed by the company's financial director in response to payment instructions received from spear phishing emails disguised to appear as if they came from the company's chief financial officer.

OUR ROLE

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.

OUR IMPACT

Our experts concluded that the client's network was not breached and that there is currently no threat of a malicious insider.

1982

Year Founded and $3.5BLN equity market capitalization*

96/100

Advisor to 96 of the world's top 100 law firms

NYSE:FCN

Publicly traded

8/10

Advisor to 8 of the world's Top 10 bank holding companies

**Number of total shares outstanding as of October 23, 2020, times the closing share price as of October 30, 2020.*

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

FTI Consulting is an independent global business advisory firm dedicated to helping organizations manage change, mitigate risk and resolve disputes: 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. **www.fticonsulting.com**

02122021 | VN01218-v06 Insider Threat Workplace (letter)

FTI CONSULTING™