Offensive Security & Stress Testing

EXPERTS WITH IMPACT™

F T I™ CONSULTING

Overview

The growing digitalization of business operations creates numerous entry points for threat actors to compromise critical systems and expose assets, data, and customer information. As these cybersecurity threats evolve and grow in impact, organizations also face pressure from regulators and stakeholders to quantify the effectiveness of cybersecurity controls in place across their systems.

Offensive security and stress testing, also known as “penetration testing,” involves simulating a malicious attack on a computer system or network to identify vulnerabilities. Our offensive security and stress testing services use the same tools, techniques, and protocols as witting and unwitting malicious actors to help identify vulnerabilities and improve security.

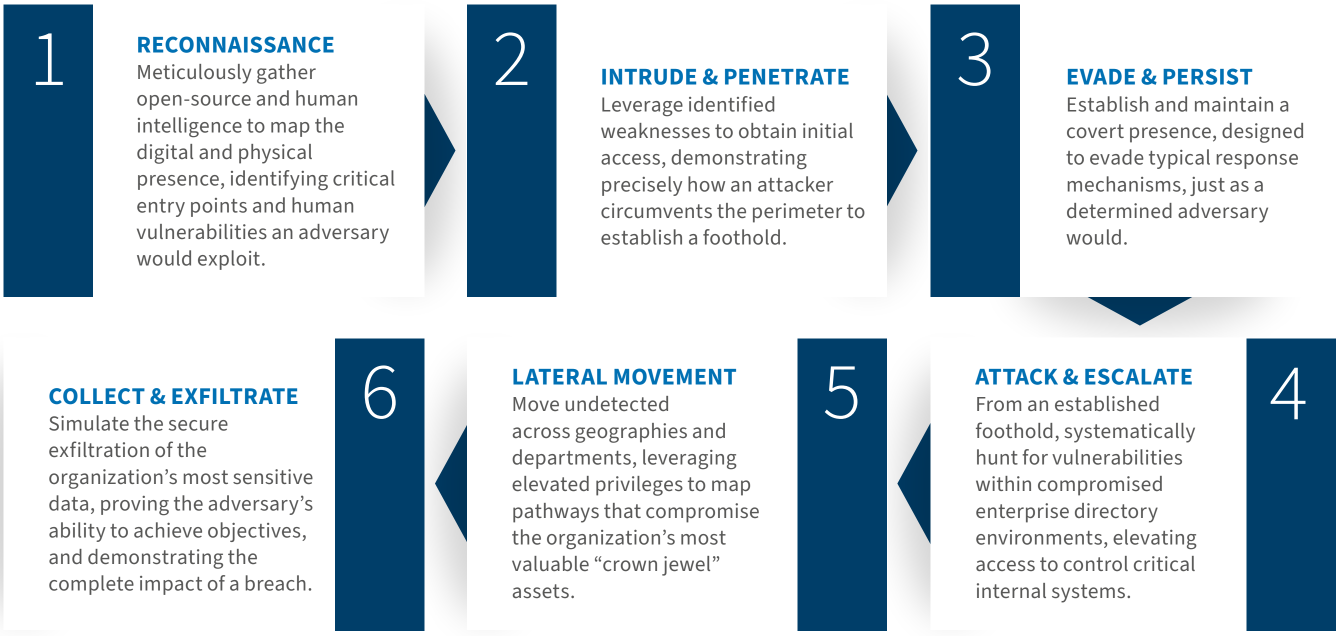
Our Expertise

Our approach to cybersecurity testing is unique because we focus on scenario-based, objective-driven tests that replicate the techniques used by real-world threat actors. Our team of experts are recognized by leading industry accreditations such as CREST; hold certifications from leading entities such as OffSec, Global Information Assurance Certification (GIAC), and SANS; and possess strong academic credentials in science, mathematics, engineering, and computer science. Additionally, the FTI Cybersecurity team has extensive experience working alongside regulators, setting requirements, and analyzing results, and has actively participated in developing threat intelligence-led penetration testing frameworks and approaches (such as CBEST, TIBER, and iCAST) for regulators and financial sector organizations.

Our offensive security and stress testing services typically help CISOs and business leaders answer the following critical questions:

- Will my company’s existing combination of security controls protect against a ransomware attack in practice?
- Do existing risk assessments, budgets, and technology transformation initiatives appropriately reflect the cybersecurity risks facing my business?
- Can my organization be breached due to security weaknesses in the supply chain or third parties?
- What data can office visitors, contractors, employees, and threat actors find on the corporate network?

Indicative Testing Stages



1

RECONNAISSANCE
Meticulously gather open-source and human intelligence to map the digital and physical presence, identifying critical entry points and human vulnerabilities an adversary would exploit.

2

INTRUDE & PENETRATE
Leverage identified weaknesses to obtain initial access, demonstrating precisely how an attacker circumvents the perimeter to establish a foothold.

3

EVADE & PERSIST
Establish and maintain a covert presence, designed to evade typical response mechanisms, just as a determined adversary would.

4

ATTACK & ESCALATE
From an established foothold, systematically hunt for vulnerabilities within compromised enterprise directory environments, elevating access to control critical internal systems.

5

LATERAL MOVEMENT
Move undetected across geographies and departments, leveraging elevated privileges to map pathways that compromise the organization’s most valuable “crown jewel” assets.

6

COLLECT & EXFILTRATE
Simulate the secure exfiltration of the organization’s most sensitive data, proving the adversary’s ability to achieve objectives, and demonstrating the complete impact of a breach.

Our Services

Our experts leverage an intelligence-driven approach to objective-based penetration testing, allowing clients to practice responding to severe situations without being exposed to the associated risks.

TotalTest Simulation

FTI Cybersecurity’s TotalTest Simulation goes beyond traditional testing, combining threat intelligence-led attack simulations with full-scale crisis response to prepare leaders for when it matters most. TotalTest helps organizations uncover vulnerabilities, strengthen defenses, and enhance crisis response capabilities.

Red Team Operations

We deliver bespoke, intelligence-led Red Team campaigns, aligned with the most rigorous global regulatory frameworks. Our multidisciplinary experts precisely emulate the tactics, techniques, and procedures (TTPs) of relevant threat adversaries, providing a definitive measure of your security program’s actual detection and response efficacy.

Purple Teaming

The Red Team works collaboratively with an organization’s Security Operations Center (SOC) to immediately expose the Blue Team to the latest adversary techniques, enabling them to build crucial context and instantly refine detection logic and response protocols. By leveraging our sophisticated attack expertise, we deliver immediate improvements, driving continuous security maturity and operational excellence.

AI Red Teaming

Our AI Red Teaming service simulates real-world adversaries targeting AI-enabled systems. By stress-testing models, data pipelines, applications, and associated integrations, we proactively identify how attackers could manipulate or extract information from AI systems. Our approach bolsters trust and safety, helping organizations confidently deploy and scale AI while staying ahead of emerging threats.

Internal Capability Program Development

We offer targeted solutions for organizations seeking to establish or enhance their internal Red Team and penetration testing operations. Our comprehensive approach focuses on developing the necessary guardrails, processes, and governance frameworks to run programs as Business As Usual (BAU). This includes crucial support for managing vendors, running pilot tests, and integrating technical standards into an effective internal capability.

Penetration Testing

Thick-Client: Our thick-client testing evaluates the security of desktop and hybrid applications that process sensitive data or connect to enterprise systems. Through controlled exploitation and behavioral analysis, we identify issues such as insecure data handling, privilege escalation, and weak updates mechanisms.

Application Programming Interface: API testing focuses on assessing how systems communicate and share information. Our team analyzes authentication authorization and data-exchange mechanisms to uncover weaknesses that could lead to data exposure or abuse.

Web Application: Web application testing combines automated security testing with manual vulnerability analysis to evaluate an application's security controls. This is done through authenticated and unauthenticated attacks to test against threat actors attempting to obtain access to sensitive data and resources.

Mobile Application: We emulate real-world adversaries targeting mobile ecosystems to assess the security posture of mobile applications across iOS and Android platforms. This comprehensive approach evaluates your apps' resilience against prevalent mobile-specific threats and developer misconfigurations.

"Assume Breach" Assessments: We evaluate a system's security posture from the viewpoint of a malicious insider or after an external perimeter breach. These assessments help system owners consider how far a threat actor could penetrate and the extent of the damage they could cause once inside the network.

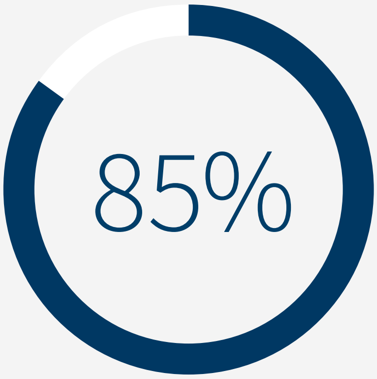
Wireless Network: Our experts can identify the risks and vulnerabilities associated with an organization's wireless network infrastructure. We assess encryption, authentication, and segmentation controls to detect misconfigurations, rogue access points, and other weaknesses that could allow unauthorized access or network compromise.

External Infrastructure Testing: External testing is enhanced by moving beyond basic scanning to a threat-informed scenario. This involves Open-Source Intelligence (OSINT) and social engineering to test the human perimeter. The goal is a highly relevant, realistic attack simulation against all public-facing assets, including cloud environments, to prove the efficacy of perimeter defenses.

Internal Infrastructure Testing: Internal testing focuses on validating controls across Active Directory (AD) and the internal network from a zero-knowledge perspective. We utilize advanced techniques to identify vulnerabilities accessible from the internal network, assessing control effectiveness against internal threats and the potential for unauthorized access.

FTI Cybersecurity's Offensive Testing Excellence

The FTI Cybersecurity Offensive Security capabilities can be summarized by our success rate. Our ability to identify, prove, and help remediate deficiencies in a client's security arrangements are evidenced by the statistics arising from our engagements:



of client environments owned in less than 12 hours

Time to Exploit

Average of **10 hours** to obtain an initial foothold in enterprise environments

Lateral Movement Success Rate

95% within AD and IT/OT environments

Vulnerability Discovery Rate

Average of 13 **critical** severity observations discovered per matter

Exploitation Success Rate

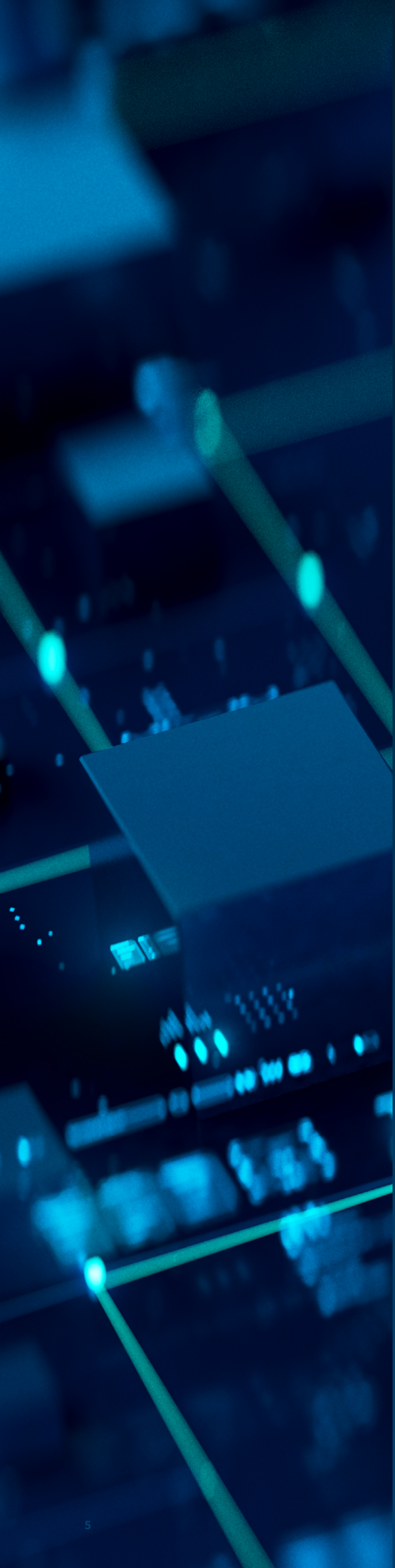
Average of 9 **critical vulnerabilities** identified and exploited per test

Time to Escalate

Median time of 7 hours to successfully escalate privileges after obtaining an initial foothold

Attack Surface Reduction

On average, **70% reduction in internal attack surface area** — via identifying and closing off attack paths



CASE STUDY

Middle East

Mobile and Web Penetration Test for a Mobile Money Operator

SITUATION

A leading telecommunications provider in the Middle East engaged FTI Cybersecurity to assess the security posture of its recently launched mobile banking platform.

OUR ROLE

Our experts conducted a full-scope penetration test. By reverse-engineering the mobile app and analyzing business logic, Application Programming Interfaces (APIs), and encryption, we uncovered vulnerabilities in the company's mobile app, web infrastructure, and associated web portals.

OUR IMPACT

FTI Cybersecurity identified a critical sequence of vulnerabilities that resulted in full compromise of the platform and exposure of customer data and funds. Our deep technical expertise uncovered flaws others missed, earning CEO praise for safeguarding critical operations.

CASE STUDY

EMEA

Red Team Assessment for a National Telecommunications Company

SITUATION

FTI Cybersecurity was engaged by a national telecommunications provider to perform a multi-month Red Team assessment designed to evaluate the organization's detection, response, and resilience against sophisticated adversaries.

OUR ROLE

Our team executed a series of coordinated attack scenarios combining technical exploitation with social engineering, including the use of AI voice-cloning and caller-ID spoofing to mirror realistic threat activity. During the engagement, we uncovered a critical systemic issue: millions of exposed SIM authentication secrets that could enable large-scale subscriber impersonation.

OUR IMPACT

The engagement delivered both immediate risk reduction and long-term strategic improvements, strengthening the client's resilience against advanced, real-world threats.

CASE STUDY

EMEA & North America

Scenario-Led Penetration Testing for a Global Private Equity Firm

SITUATION

A global private equity firm engaged FTI Cybersecurity to perform internal penetration testing to ensure timely preparedness for a significant cyber attack.

OUR ROLE

Our Offensive Security team was able to bypass enterprise security technologies such as privileged identity management, endpoint threat detection, and response controls to compromise several employee and server administrator accounts. Within four hours we had gained full control over the client's global enterprise environment.

OUR IMPACT

We identified several weaknesses that could be used by threat actors to install ransomware, facilitate fraud, share sensitive information, or cause operational outages. We conducted all testing without impacting regular business operations.

CASE STUDY

EMEA & North America

TotalTest Simulation for a Global Law Firm

SITUATION

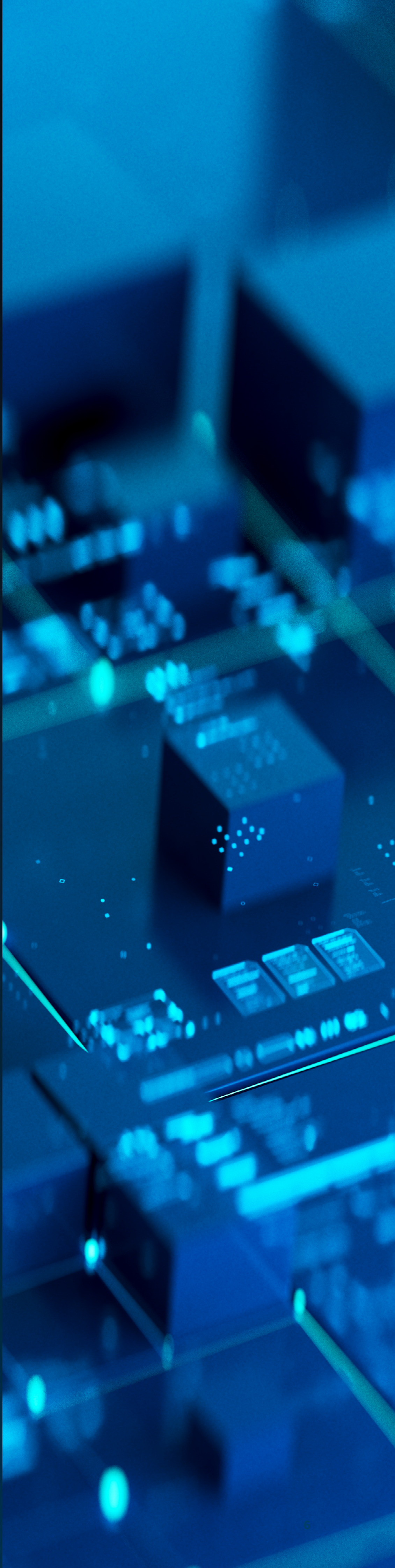
A global law firm engaged FTI Cybersecurity to conduct a TotalTest Simulation to gain a more detailed understanding of their cyber resilience capabilities.

OUR ROLE

Our approach combined external and internal penetration testing, social engineering, and tailored tabletop exercises to assess technical defenses, employee awareness, and leadership response. This holistic approach provided a comprehensive evaluation of the law firm's cybersecurity resilience and crisis readiness.

OUR IMPACT

The TotalTest Simulation allowed the firm to rehearse their response to highly relevant attack scenarios in a safe and controlled environment, identifying strengths and weaknesses in their processes. This approach fostered a collaborative and proactive security culture across the organization.



CASE STUDY

Taiwan

Penetration Test for a Multinational Renewable Energy Producer in Taiwan

SITUATION

FTI Cybersecurity was engaged by a renewable energy company to complete a red flag assessment at a Taiwanese solar farm, part of a portfolio of 450 solar parks in the region.

OUR ROLE

We conducted a targeted assessment and penetration test in Taiwan, evaluating the organization's operational technology security. The team tested device firmware integrity, network communications, and credential protection, simulating rogue base station attacks and custom firmware deployments to identify critical vulnerabilities.

OUR IMPACT

Our testing revealed the absence of security checks within the organization's network, which could allow the installation of custom firmware by threat actors. FTI Cybersecurity provided actionable recommendations to enhance security maturity across all 450 solar parks.

CASE STUDY

China

IoT Penetration Test for a Surveillance Equipment Manufacturer

SITUATION

FTI Cybersecurity conducted penetration testing on a Chinese state-owned manufacturer's products to support legal efforts to prevent exclusion from sensitive government locations in the UK.

OUR ROLE

Our team determined that the security systems evaluated were free of embedded backdoors and intrinsic weaknesses that might permit remote access without authentication.

We held regular client briefings to share insights, pinpoint critical improvement areas, and tackle potential vulnerabilities that could compromise their stance.

OUR IMPACT

In under a day, our experts helped the firm quickly and reliably identify the root cause of weaknesses and upgrade their product line to be prepared for ongoing legal discussions with the UK government.

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

- Comprehensive services include crisis communications, e-discovery, forensic investigations, and more
- Seamless integration of FTI Consulting's expertise across service offerings

Key Benefits

- Communicate security vulnerabilities within your organization to stakeholders and develop effective strategies to defend against real-world attacks, improving breach preparedness.
- Evaluate the effectiveness of security tools, technology, and processes through tailored, scenario-based controlled incidents.
- Identify gaps in incident response plans and build a remediation plan to address root cause issues, reducing risk exposure across the enterprise.
- Rehearse and prepare people, processes, and tools to respond to cyber attacks, building "muscle memory" for quick response.
- Assess employee response to real-world threats and provide targeted training to proactively identify and respond to security threats in a timely manner.

1982

Year founded

8,300+

Employees worldwide

800+

Senior Managing Directors

34

Offices in 34 countries and territories around the globe

817

Ranked 817 on the Fortune 1000

100

Advisor to all 100 of the world's top 100 law firms as ranked by *The American Lawyer* Global 100 list

90

Advisor to 90 of the Fortune 100 corporations

71

Advisor to 71 of the top 100 private equity firms as ranked by the Private Equity International 300 list

Client group statistics are based on data from January 1, 2024, through December 31, 2024. All other statistics above are as of December 31, 2024.

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 20 3077 0466
david.dunn@fticonsulting.com

Nebu Varghese
Senior Director
+44 20 3077 0230
nebu.varghese@fticonsulting.com

EXPERTS WITH IMPACT™