Cybersecurity
Private Equity Services

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

All organizations are vulnerable to cybersecurity risk. Private equity firms face the dual challenge of preparing for threats to their organization and their current and future portfolio companies. With the potential for millions of dollars in damages and significant reputational implications, it is a risk worth preparing for. FTI Cybersecurity works with your team to evaluate your specific needs to tailor solutions that enhance security and resilience against the unique cybersecurity risks facing your organization and your potential investments.

— CYBERSECURITY PRIVATE EQUITY SERVICES

— Transaction Services

— Portfolio Company Cybersecurity Assessment Program (PCCAP)

— Transformation Services

— Incident Response Retainer

Transaction Services

The cybersecurity and IT aspects of M&A transactions have become one of the most pervasive, complex, risky, and, at times, expensive activities to address. Our cybersecurity experts work throughout the transaction lifecycle, delivering due diligence, integration synergy assessments, roadmaps, program management, carve-out planning, transition management, and buy-side and sell-side support.

Cybersecurity Due Diligence

We identify and report on cybersecurity strengths, weaknesses, and threats as part of our due diligence during transactions. We also identify future opportunities and requirements to reduce risks, improve capability, and add enterprise value. We deliver tailored reports, from high-level "red flag" risk assessments to deep thesis-based analyses, with value-creation recommendations and one-time and run-rate cost models.

Merger Integration

Our team of experts identifies and quantifies cybersecurity merger integration synergies and value-creation opportunities. We help define an appropriate future cybersecurity environment and design a roadmap to transition from current state to future state. We manage cybersecurity and IT integration programs at all stages and levels, including pre-close preparation, day-one execution, and 100-day program management of internal and third-party resources.

Carve-outs

We provide a holistic and comprehensive understanding of key cybersecurity, regulatory, entanglement, staff, and technology drivers that may directly impact value and present future operational challenges. Our team also supports transition service agreement (TSA) development, negotiations, standup, and testing, as appropriate. We also develop stand-up roadmaps and provide interim Chief Information Security Officer (CISO) and IT leadership to ensure experienced guidance and execution throughout the process.

IPO Readiness

Ahead of an IPO, our team assesses a company's readiness to go public by ensuring best practices and controls are implemented and identifying any cybersecurity risks and the critical gaps that should be remediated immediately, given the heightened impact on public companies. Our team will ensure that key components of a cybersecurity program are in place and operating effectively prior to the IPO.

EXPERTS WITH IMPACT™

FTI CONSULTING™ | CYBERSECURITY

Portfolio Company Cybersecurity Assessment Program (PCCAP)

Our PCCAPs are ongoing programs which assess the maturity and risk across a private equity firm's investment portfolio, as well as, work at the individual portfolio company (portco) level to improve maturity and reduce risk. This program embodies a proactive approach, ensuring that portfolio companies are fortified against potential vulnerabilities and cyber attacks. PCCAPs bring forth a comprehensive and tailored assessment, delving into the intricacies of each portfolio company's cybersecurity infrastructure and providing a firm valuable insight into the effectiveness of implemented measures and the impact of new emerging threats.

Our PCCAP offering allows portcos to be assessed based on a standardized framework and monitored and reviewed on a recurring basis. These assessments are customizable based on the private equity firm's needs and include maturity assessments at their core. By evaluating the maturity of security protocols, these assessments not only identify strengths and weaknesses but also provide a strategic roadmap for continuous improvement. This approach ensures that portfolio companies not only meet industry standards but foster a culture of ongoing enhancement and innovation in their cybersecurity practices.

Our service offering also includes assessment of information on the dark web as well as identification of open web vulnerabilities, providing private equity firms and portcos with a view of potentially exploitable risks and vulnerabilities. These assessments provide an "outside-in" view to demonstrate what an attacker may see and exploit. In support of these assessments, our team provides remediation advice, where required.

Benefits include:

— Visibility of risk across the portfolio

— Prioritized strategy and investment roadmaps

— Reduced likelihood and impact of cybersecurity breaches

— Protection and increased value of portfolio companies

— Ensure effectiveness and risk-based investment in cybersecurity

Additional services include:

— Risk Assessments: Using a company's current cybersecurity posture and potential risks, FTI provides a viewpoint into the most critical and imminent threats.

— Penetration Testing: By simulating real-world attacks, penetration testing validates the effectiveness and configuration of security controls, which provides an additional layer of assurance.

— Application Security Assessments: Assessing applications and development practices helps ensure that the products have robust security measures, reducing potential risks and providing assurance to external parties.

Transformation Services

Our Advisory and Transformation services effectively change the landscape of cybersecurity programs through intelligence-led, expert-driven, strategic solutions that map gaps across organizations, produce achievable roadmaps, and implement innovative cybersecurity programs of the future that drive business value, enable growth, and increase resilience.

Governance, Risk, and Compliance Programs

We support organizations central coordination and oversight of security operations through policy development, vCISO services, resilience planning, and training programs.

Intelligence & Testing

Our team conducts threat hunting, compromise assessments, threat intelligence, vulnerability assessments, and penetration testing to proactively identify and mitigate existing and potential threats.

Digital & Technology Transformation

We support organizations with securely enabling technology roll-outs, cloud migrations, infrastructure virtualization, and convergence through subject matter expertise support and strategic planning.

Data Privacy & Management

We support clients with assessing and managing the regulatory landscape and provides data privacy advisory and managed services. We also support organizations with identifying privacy risks, red flags, and proposed remediations.

Incident Response Retainer

Our Incident Response (IR) Retainer provides immediate access to advice and support from our expert Incident Response consultants whenever an incident occurs. Our pre-defined agreement provides peace of mind, removing the need to negotiate terms and sign potentially complex contracts in the middle of an incident.

Base Support

Our Base retainer provides the basic coverage with a focus on reactive service offerings. The included 64 prepaid hours ensures you are covered during the initial triage and response phase of an incident, enabling you to focus on your business priorities. This base retainer also includes information sharing and intelligence briefings.

Essential Support

Ensuring readiness for cyber threats is not just crucial but imperative for the success of your incident response program. We recognize the significance of preparedness, and that is why we include information sharing, intelligence briefings, IR First Responders training, and cyber incident response simulations.

Advanced Support

The Advanced retainer is designed to assess your organization's specific requirements, gain a comprehensive understanding of the incident response maturity level, and help build a roadmap for improvement. This ensures optional preparedness to respond effectively in case of an attack. This includes information sharing, intelligence briefings, IR First Responders training, cyber incident response simulations, and IR maturity roadmap development.

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

Services include crisis communications, e-discovery, forensic investigations, and more

Seamless integration of FTI Consulting's expertise across service offerings

---

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

BRAD CARPENTER
Managing Director
+1 908 507 6818
brad.carpenter@fticonsulting.com

FTI CONSULTING