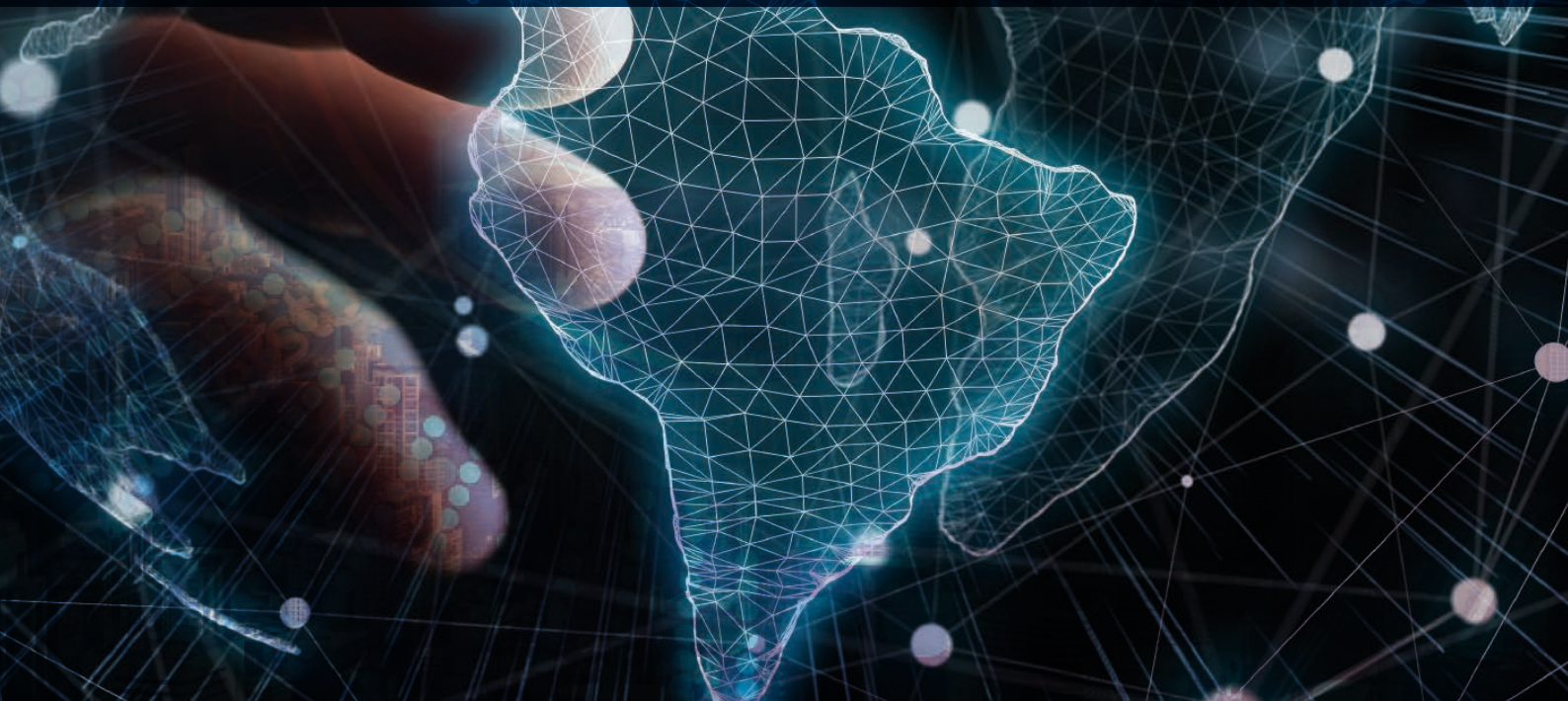
Cybersecurity
Private Equity Services

FTI CONSULTING™

EXPERTS WITH IMPACT™

We are a global leading provider of independent cyber and risk management advisory services with a core offering focused on cyber readiness, incident response, and complex investigations.



Cybersecurity Private Equity Services

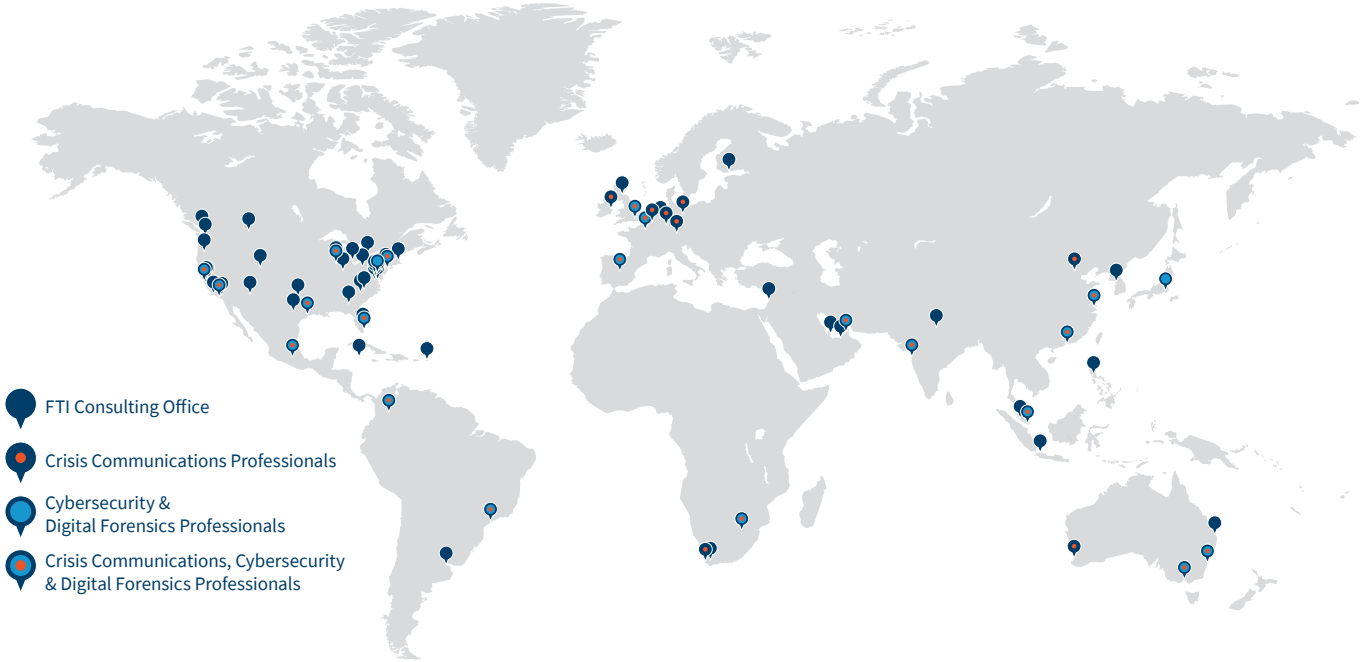
All organizations are vulnerable to cybersecurity risk. Private equity firms face the dual challenge of preparing for threats to their organization as well as their current and future portfolio companies. With the potential for millions of dollars in damages and significant reputational implications, preparing for this risk is vital.

We are a global leading provider of independent cyber and risk management advisory services with a core offering focused on cyber readiness, incident response, and complex investigations.

As an international company with clients across the globe, we help organizations understand their own environments, harden their defenses, respond to crises holistically, and recover operations and reputation after an incident. Our team has a unique ability to include sector and industry expertise alongside our cybersecurity capabilities.

A Global Team, Intelligence-led, Expert-driven

Our team, capable of deploying worldwide, consists of more than 450 dedicated cybersecurity experts, incident response consultants, developers, and data analysts with extensive investigative backgrounds, led by those with decades of experience at the highest levels of law enforcement, intelligence agencies, and global private sector institutions.



The FTI Cybersecurity Difference

Cybersecurity strategy, incident response, transaction engagement, and investigations for private equity firms and their portfolio companies carry considerations in addition to cyber. FTI Consulting supports all interconnected needs and challenges, such as comprehensive transaction and transformation services, forensic accounting, data analytics, data privacy and information governance, crisis management and strategic communications, complex interdisciplinary investigations, and fraud and anti-money laundering. We have comprehensive expertise spanning nearly every industry.

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

Cyber Readiness for Private Equity Firms & Portfolio Companies

FTI Cybersecurity works with your team and your portfolio companies to evaluate specific needs to tailor solutions that enhance security and readiness to defend against the unique cybersecurity risks facing your organization and your investments.

Assessments

To ensure your organization and portfolio companies are properly protected, our experts perform cybersecurity program assessments; vulnerability assessments; and policies, procedures, and staff gap analysis and design. Our team will determine if you and your investments meet industry standard best practices, identify and assess vulnerabilities, and devise a holistic set of scored recommendations.

Penetration Testing & Red Teaming

Our team leverages multiple methodologies for identifying cyber risk. Penetration testing simulates an attacker with and without familiarity of your infrastructure and tests systems for weaknesses. Red teaming allows our experts to test your intruder detection defenses, simulate what would happen in a real cyber attack, and provide your team with relevant experience on what to look for and how to react.

Threat-hunting Operations

Threat-hunting operations actively search for and detect threats, allowing for remediation before warnings are triggered. Our experts can assist private equity firms by using an innovative approach that fuses operational intelligence and cybersecurity technical intelligence and engaging in operations that focus on likely targeted areas of your network, or of your portfolio companies, to proactively identify advanced persistent threats.

Crisis Simulation & Table-top Exercises

FTI Cybersecurity offers custom exercises designed to test and improve your organization's capabilities to respond to cybersecurity events. We use real-world scenarios that can build from a workshop to a full simulation depending on your resilience maturity. We focus on functional teams, provide technical realities, and run multi-organization, multi-day cross-functional crisis simulation exercises.

Information Governance, Privacy & Security

Exploding growth of corporate data, whether stored on servers, in the cloud, or on employee devices, presents new challenges and opportunities for your private equity firms. Our Information Governance, Privacy & Security experts can: Develop and implement information governance solutions that reduce corporate risk, cut storage costs, secure data, implement data loss prevention strategies, improve the e-discovery process, and enable faster and deeper insight into data.

Cybersecurity Compliance for Portfolio Companies

Our experts focus on ensuring that your organization meets its unique compliance requirements while maximizing the return on cybersecurity investment. Our cybersecurity compliance services address: GDPR, NY DFS, PCI DSS, and CCPA.

Dark Web Intelligence & Monitoring

Our team performs an initial dark web assessment to identify existing compromises that could make you and your assets less secure. Further, our experts can maintain reoccurring dark web monitoring to inform the client if any new breaches occur.

Cybersecurity Protection for High-profile Individuals

Reliance on mobile devices and home offices to conduct business has become more prevalent, and malicious actors take advantage of new entry points to access information and capital. Using the experience gained by defending Fortune 100 companies, we assist individuals with the same service right in their home.

Employee Training

Using extensive industry experience, our experts design programs that build your employees' knowledge base, define appropriate standards of conduct, and promote secure behavior.

Board Level Advisory

Our experts inform and enlighten Boards regarding their unique cyber risk profile in a non-technical manner. This clear guidance allows for a streamlined decision process for mitigating threats and facilitates efficient communication with the C-suite and those responsible for implementation.

CASE STUDY

CYBERSECURITY ASSESSMENT FOR A GLOBAL PRIVATE EQUITY FIRM

SITUATION

A global private equity investment firm was undergoing a transformation of its cybersecurity program and needed a formal, independent assessment of its cybersecurity maturity level.

OUR ROLE

Our team was hired to conduct a comprehensive cybersecurity program assessment that included a review of policies, procedures, staff, technology, and established controls. The assessment lasted approximately three weeks and required detailed staff interviews, site visits, and significant document review.

OUR IMPACT

Our experts identified several gaps in controls, written policies, and procedures. We produced a detailed roadmap allowing the client to properly align with industry standards and best practice frameworks, and to remediate gaps quickly and effectively without a significant expansion of its budget. This resulted in an immediate improvement to the client's cybersecurity maturity level score.

Custom Portfolio Company Cybersecurity Assessment Program

While many private equity firms have invested wisely in assessing cybersecurity risks at portfolio companies, establishing a defined process to identify and fill existing gaps will allow for proper hardening of portfolio cybersecurity postures and greater insight into risk across the portfolio.

FTI Cybersecurity's bespoke assessment program scores and monitors the cybersecurity maturity level of portfolio companies to provide detailed insights for private equity clients on the following:

- Strength of each portfolio company's cybersecurity program
- Level of cyber risk each portfolio company faces
- Key areas of improvement needed to close critical gaps in each portfolio company's cybersecurity program
- Confirm if recommended improvements have been properly implemented
- Analyze and model change in portfolio maturity scores over time

Assessment Program Components

- Customized web-based dashboard and central repository for PE firm and portfolio company access
- Compartmentalized access for PE firm and portfolio companies
- Individual pages for each portfolio company
- Custom designed cybersecurity maturity assessment framework and scoring system built upon the most respected industry standard best practices
- Easy to use, bespoke assessment scorecards, detailing target maturity levels for each portfolio company, cybersecurity control areas scores, and a scored set of risk and impacts identifying impact potential to a portfolio company due to data loss, insider threat activity, disruptive attacks, destructive attacks, and fraud
- Address portfolio company preparedness for ransomware, business email compromise, insider threats, distributed denial-of-service (DDoS) attacks
- Chronologic, priority-based roadmap of hardening measures for each portfolio company
- Cost effective remediation and identification of gaps
- Ongoing monitoring and updated scoring: Re-assessment, hardening measures check-up
- A suite of cyber readiness and IT consulting services that can be added to portfolio company assessments, or specified by portfolio companies, including:
  - vulnerability scanning
  - threat hunting
  - penetration testing
  - data privacy and information governance
  - virtual chief information security officer
  - IT modernization
  - secure digital transformation

CASE STUDY

PORTFOLIO CYBERSECURITY ASSESSMENT FOR A LEADING PRIVATE EQUITY FIRM

SITUATION

After a series of cyber attacks to its portfolio companies, a global private equity firm with over $50bn in commitments wanted to institute a program to map risk across their portfolio, and improve the cybersecurity programs of its portfolio companies, by ensuring critical controls were implemented.

OUR ROLE

Our team designed and established a Portfolio Company Cybersecurity Assessment Program, which detailed the cybersecurity process required during the investment lifecycle, and ensured implementation of key policies and practices at the portfolio company level. We used a custom-built framework and scoring methodology based on industry standards.

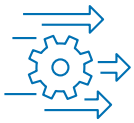
OUR IMPACT

Our expert's work led to significant cybersecurity improvements to all portfolio companies included in the program, allowing them to better defend against threats and effectively plan for future needs. Further, we provided critical information to the client's deal and portfolio operations teams, and to the portfolio companies themselves.

Transaction & Transformation Services

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 and program management; and carve-out planning, transition (TSA) management, and buy-side and sell-side support.



Responsiveness

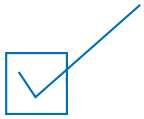
We recognize the often-urgent timelines associated with deal cycles, and the need to provide timely, quality answers.

Technical Depth

We have a globally recognized team of experts spanning all domains of cybersecurity across industry and government.

Global Reach

We operate with 107 offices in 82 cities across the globe, delivering multi-lingual due diligence engagements in a seamless manner.



Quality and Impact of Output

We focus on the business requirement, ensuring our outputs answer the exam question.

Complementary Breadth

We have an integrated and comprehensive approach which embeds cybersecurity with our related segments including Corporate Finance, Strategic Communications, and Forensic Investigations.

Cybersecurity and IT Due Diligence

We identify and report current cybersecurity and IT strengths, weaknesses, and threats, as well as future opportunities and requirements to reduce risks and costs, improve capability and service delivery, 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

We identify and quantify cybersecurity and IT-enabled merger integration synergies and value-creation opportunities. FTI Cybersecurity helps define an appropriate future cybersecurity and IT 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/vendor resources.

Buy Side Carve-outs

In today's threat and technology landscape, assessing the key cybersecurity and IT risks and components needed to properly stand-up and successfully operate a carved-out business is paramount in every deal. FTI provides a holistic and comprehensive understanding of key cybersecurity, regulatory, entanglement, staff, and technology drivers that may directly impact value and present future operational challenges. We also develop stand-up roadmaps and provide interim a Chief Information Security Officer and IT leadership to ensure experienced guidance and execution throughout the process.

CASE STUDY

RED FLAG CYBERSECURITY & IT DUE DILIGENCE FOR A CUSTOM WINDOW MANUFACTURER & INSTALLER

SITUATION

A private equity client was considering an acquisition of a $200M custom window manufacturer and installer and in order to protect their investment, wanted to identify and quantify IT risks, weaknesses, and opportunities, and understand additional IT investments needed.

OUR ROLE

Our team interviewed and collected artifacts from executives and IT management to understand IT requirements and environment; assessed IT organization, applications, infrastructure, security, compliance, budget, and spend; and assessed in-flight ERP System Implementation, to determine feasibility of timeline and costs.

OUR IMPACT

Our experts identified numerous cybersecurity vulnerabilities and PII and PCI Compliance issues, and prepared a remediation plan. Our team was subsequently engaged by Target to manage remediation. The Target remediated red flags and the Private Equity Client successfully acquired the Target.

Sell Side Carve-outs

FTI Cybersecurity identifies the cybersecurity and IT components that need to be divested with the carved-out business. We examine the degree of cybersecurity and IT systems and data entanglement, and define the support, separation, and TSA approach, activities, timing, and costs. We manage all aspects of cybersecurity and IT carve-out programs, including TSA compliance and exit, contract novation, and internal and third-party vendor resources.

Carve-Out Services Include:

- Virtual Chief Information Security Officer (vCISO)
- Future-State Design, Plan, and Implementation
- Vulnerability Assessment, Penetration Testing, and Threat Hunt Operations
- Regulatory Alignment
- Data Management and Governance
- Data Separation and Migration
- Cybersecurity and Business Applications Separation
- Infrastructure Separation and Transition
- TSA Development and Management
- Outsourced Cybersecurity Monitoring
- Digital Operations Transition

Transformation Offerings

A strong, proactive cybersecurity program is critical in a world where cyber threat actors continue to become more sophisticated, the number of cyber-attacks increase, companies evolve toward digital business models, and cybersecurity and data privacy regulatory requirements become more demanding.

FTI helps clients transform their cybersecurity programs to effectively meet this changing landscape 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.

Cybersecurity Transformation Services include:

- Holistic Cybersecurity Program Assessment and Implementation
- Virtual Chief Information Security Officer (vCISO)
- Cybersecurity Fusion Center and Security Operations Center (SOC) Design
- Data Privacy and Information Governance Transformation
- Regulatory Compliance Alignment
- Technology Modernization
- Enterprise Data Management and Data Lakes
- Cloud Migration
- IoT and Blockchain
- Bespoke Applications

CASE STUDY

SECURITY & TECHNOLOGY PROGRAM TRANSFORMATION FOR A MAJOR SUPERMARKET CHAIN

SITUATION

FTI Cybersecurity was engaged to investigate a business email compromise attack.

OUR ROLE

Our team determined that direct system access occurred and an IT administrator's account had been compromised. After disabling the administrative privileges, FTI Cybersecurity monitored the account for critical insights and intelligence to give to law enforcement.

OUR IMPACT

FTI Cybersecurity was further retained to investigate an internal sensitive data exposure. We identified employees accessing the data and investigated for malicious intent. We are also providing an interim Chief Information Officer to spearhead the transformation of the client's security and technology program, and security operations resources to assist with monitoring. Additionally, FTI has developed and led an extensive corrective action plan to address the security gaps.

CASE STUDY

RED FLAG CYBERSECURITY & IT DUE DILIGENCE FOR A HEALTH INSURANCE PROVIDER & ADMINISTRATOR

SITUATION

A private equity client was considering an acquisition of a health insurance provider and administrator and wanted to identify and quantify any IT risks, in order to protect their investment, understand any additional IT investments needed, and capitalize on IT-enabled value creation opportunities.

OUR ROLE

FTI Cybersecurity interviewed and collected artifacts from executives and IT management to understand IT requirements and environment; assessed IT organization, applications, infrastructure, security, compliance, budget, and spend; assessed proprietary claim analysis and rating system, to determine capability, stability, security, compliance and scalability; and current IT managed services provider (MSP) services, capabilities, and contracts.

OUR IMPACT

Our experts identified numerous cybersecurity vulnerabilities and PHI compliance issues, and red flags related to the MSP's infrastructure platform and network connectivity selection, maintenance, and support. Our team prepared a remediation plan and after the red flag issues were addressed, the private equity firm acquired the target company.

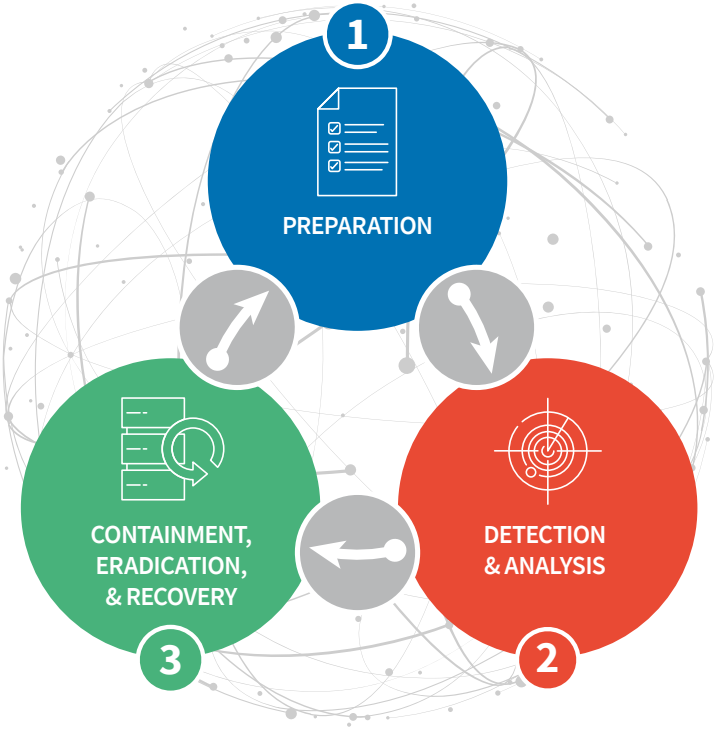
We provide complete cyber incident response solutions that include planning, analysis, mitigation, system refinements, and ancillary mission support functions, such as strategic communications and reputation management.

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.

Whether it's ransomware, business email compromise, a trusted insider, or foreign actor, we provide complete cyber incident response solutions, including preparedness and response planning, incident response, analysis, identification, containment, eradication, mitigation, system refinements, and ancillary mission support functions, such as crisis management, strategic communications and reputation management.

Cyber attacks and other critical security incidents can impede your ability to keep your business moving. We help clients get to the bottom of what happened and limit additional damage. We focus on each phase of the incident response life cycle to deliver tailored plans that meet your organization's needs. This custom application of fundamental incident preparedness and response components maximizes your organization's efficiency and effectiveness when dealing with an incident. Clients rely on us to help them at every stage of the incident response life cycle.



Type of incidents we respond to:

- Ransomware
- Data breaches
- Insider threats
- Business email compromise
- DDoS attacks

Incident Response

Preparation

Being ready for cyber threats is fundamental to the success of your incident response program. This phase involves establishing and training an incident response team and developing appropriate tools and resources you will need for each aspect of incident response. We work with your business to select and implement controls based on the results of our risk assessments to limit the number of potential incidents your organization may face.

Detection & Analysis

Residual risk inevitably persists after controls are implemented. Early steps to identify, detect, and analyze threats facing your networks are key to developing effective containment and eradication strategies. Once an incident is identified, we combine the resources and tools necessary to determine the scope, impact, and appropriate response. These efforts determine the source of the incident and preserve necessary forensic artifacts.

Containment, Eradication & Recovery

This phase of incident response seeks to prohibit data from leaving networks and prevent further damage. Eradication is the removal of malicious code, actor accounts, or unnecessary access, as well as repairing vulnerabilities that may be the root cause of the incident. Once the incident has been contained and eradicated, recovery can begin. Through a post-incident assessment, we detail the cost, cause, and response for the incident, along with steps that should be taken to prevent future incidents.

E-discovery

We provide end-to-end e-discovery services globally, using leading e-discovery technology, expert teams, and innovative workflows to help clients quickly and cost-effectively understand the matter and develop case strategy.

Data Identification & Document Review

Data breaches can have long-lasting effects on a business if they are not properly remediated. We regularly conduct reviews in multiple formats and languages, and our expertise ensures important information is not overlooked, allowing for remediation, regulation compliance, and accurate document preparation.

In-bound Call Center & Notifications

We can set up an in-bound call center with unique phone numbers in over 30 languages. Our team handles the call center setup, training of staff, and escalation of issues, allowing your organization to focus directly on handling the breach itself. We also provide notification services depending on the need of the organization.

Crisis Management & Strategic Communications

Effective management coupled with internal and external communication is imperative during any cybersecurity event – from a business email compromise to a ransomware attack threatening full extinction.

When stakes are high, we provide strategic counsel to clients in sensitive situations with legal, financial, regulatory, and reputational implications by developing your communications strategy, mapping stakeholders and audiences, and developing messaging materials.

CASE STUDY

RANSOMWARE INCIDENT RESPONSE FOR A BILLING & FINANCE SOFTWARE PROVIDER

SITUATION

At 3:00AM on a Saturday morning, our Client received critical alerts of a problem with their network. The Company was hit by a sophisticated ransomware attack that encrypted of their servers and halted critical business operations.

OUR ROLE

Within hours of approval, FTI Cybersecurity boarded a flight to the Client's office. Immediately upon arrival, we started hardware imaging and analysis to determine the strain of ransomware and available options. Although the ransomware was quickly identified, there was no known way to quickly decrypt the files, it was decided to begin negotiations for payment. Despite the Client's preparedness to pay the full ransom, we worked with our Strategic Communications team to craft a plan to negotiate a lower fee.

OUR IMPACT

Our experts successfully negotiated a reduced ransom, saving the Client significant amounts of money. We worked on this engagement around the clock for close to three days, until the decryptor was obtained and the servers were once again successfully online.

CASE STUDY

RANSOMWARE INCIDENT RESPONSE FOR A GLOBAL AEROSPACE MANUFACTURER

SITUATION

FTI Cybersecurity was hired to assist a major aerospace manufacturer with a ransomware attack which brought operations to a halt. Eight of the company's locations were impacted requiring geographically disparate IT teams to work in concert to restore business operations. Additionally, the client had legacy hardware connected to the network, which posed remediation risks.

OUR ROLE

Our team was onsite at impacted locations within 24 hours. Initial response focused on identifying the malware, performing forensic review, and liaising with law enforcement. Given the client handled Controlled Unclassified Information, we determined that information was accessed. We also identified the threat of legacy equipment and worked to remove these devices. FTI also identified manufacturing machines connected to the corporate network with vulnerabilities. We created stopgap plans to isolate these machines and avoid reinfection risk.

OUR IMPACT

Due to the complexity of the existing infrastructure, had legacy workstations not been isolated, reinfection was a virtual certainty. We designed procedures to securely restore IT servers across multiple locations and remained on-site until systems were safely up and running. Our work significantly reduced overall downtime.

Cybersecurity Assessment & Incident Response Retainer

Our Cybersecurity Assessment and Incident Response Retainer provides recurring cyber readiness services to identify vulnerabilities, harden gaps, and stay ahead of the curve, coupled with dedicated incident response services that can be rapidly deployed to any global location.

From monthly fixed fee to no-cost retainers, we work with your team to evaluate the specific needs of your organization and tailor solutions that enhance security and resilience against the unique cybersecurity risks facing your organization.

Standard Retainer Services

- No up-front cost to retain FTI
- 24/7 access to incident response hotline
- Initial contact within four (4) hours

Partner Retainer Services

- Dedicated incident response & investigative services
- Regular vulnerability assessments & penetration testing
- Flex hours to be used as needed
- Cybersecurity network defense & internal controls audit
- Policy review & design
- Threat-hunting operations
- Incident preparedness & response planning
- C-suite & board advisory
- Table-top exercises
- Employee training

CASE STUDY

CYBERSECURITY RETAINER FOR A PRIVATE EQUITY FIRM

SITUATION

A large private equity firm retained FTI Cybersecurity to provide expert guidance, technical work, and dedicated incident responses services on an ongoing basis.

OUR ROLE

Our team designed a custom, retainer-based model to provide dedicated global incident responses services; regular vulnerability assessments, penetration testing, and custom training for all staff.

OUR IMPACT

FTI's work has significantly improved the cybersecurity controls for the client, increased staff awareness, and provided a flexible, cost-effective resource to tackle cybersecurity and IT challenges.

About FTI Consulting

OUR COMPANY

With over **6,250** employees and offices in **28 countries** on six continents, our breadth and depth extends across every major social, political, and economic hub **around the globe**

Founded in **1982** and **$3.5BLN** equity market capitalization*

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

53 of the **Global 100 corporations** are clients

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

OUR EXPERTISE

Trusted advisors serving clients globally with **diverse expertise** and **exceptional credentials** including accountants, economists, engineers, former CFOs, and strategists

We are a **global advisory firm** that provides multi-disciplinary solutions to **complex challenges** and **opportunities**

Expertise across a range of industries:

- Construction
- Energy Power & Products (EPP)
- Financial Services
- Healthcare & Life Sciences
- Insurance
- Mining
- Real Estate
- Retail & Consumer Products
- Telecom, Media & Technology (TMT)

We combine unparalleled **expertise** and **industry knowledge** to address critical challenges for clients

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

GLOBAL

ANTHONY J. FERRANTE
Senior Managing Director
Global Head of Cybersecurity
ajf@fticonsulting.com

ASIA PACIFIC

MASON DREW
Managing Director
Singapore
mason.drew@fticonsulting.com

AMERICAS

JORDAN RAE KELLY
Senior Managing Director
Head of Cybersecurity, Americas
jordan.kelly@fticonsulting.com

DAVID DUNN
Senior Managing Director
david.dunn@fticonsulting.com

EUROPE, MIDDLE EAST, INDIA, AFRICA

DAVE HARVEY
Managing Director
United Kingdom
dave.harvey@fticonsulting.com

THOMAS HUTIN
Senior Managing Director
France
thomas.hutin@fticonsulting.com

EXPERTS WITH IMPACT™

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.

FTI CONSULTING™