FTI Cybersecurity

An intelligence-led, expert-driven, strategic approach to global cybersecurity challenges

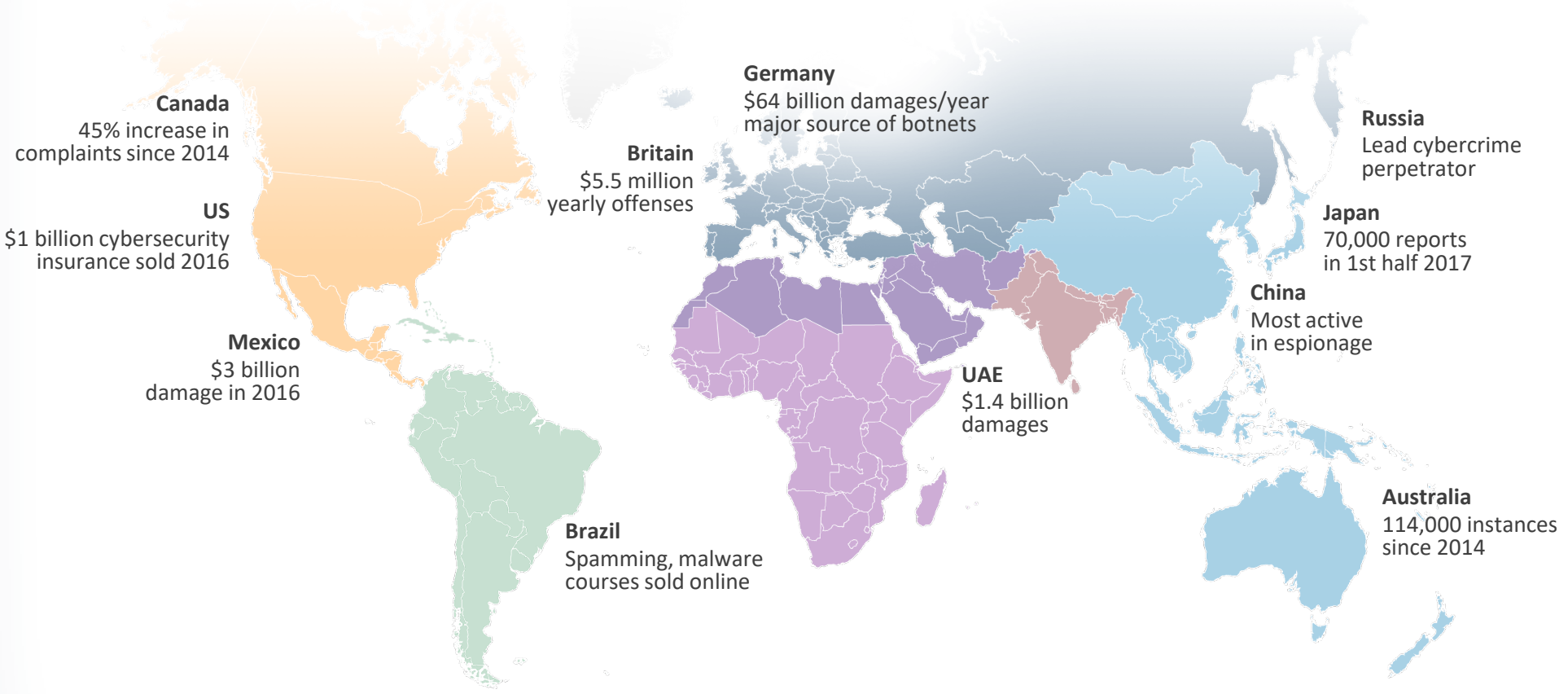
FTI Cybersecurity

Cyber Threats Overview

Cybercrime: A Global Epidemic

Cyber crime highlights

Economic impact: McAfee report, February 2018
Estimated annual global cost: $600 billion



North America	Latin America & Caribbean	Europe & Central Asia	Mid East & North Africa	Sub-Saharan Africa	South Asia	East Asia & Pacific
$157B	$22.5B	$170B	$3.5B	$2B	$11B	$160B

FTI CONSULTING
CYBERSECURITY

Current State of Play

We are creating significantly more **entry points** for attackers

Cyber criminals are extremely sophisticated and getting better

Hackers are not bound by **borders, laws or moral code**

Cryptocurrency has provided the ability to monetize cybercrime efficiently and anonymously

Information is being **weaponized**

FTI CONSULTING

CYBERSECURITY

Nature of the Threat Today

Complex, global, and constantly **changing**

Perpetrated **remotely**

Difficult to **trace**

Massive business **impact**

FTI CONSULTING

CYBERSECURITY

Who's Behind All of This?

Hacktivist

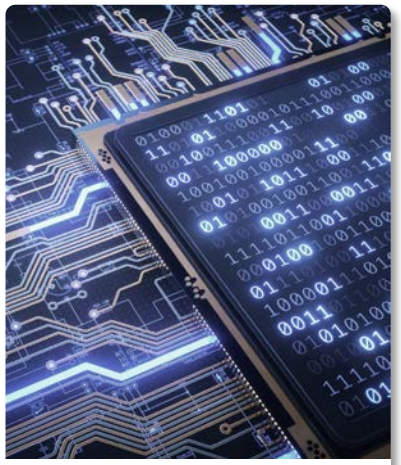
Exploit corporate and government computer networks to advance their political or social causes.

Cybercriminals

Are primarily motivated by money and stealing data to be sold on the black market.

Nation State Actors

Leverage cyber operations to achieve strategic objectives on the world's stage.



Advanced Persistent Threats

Possess sophisticated levels of expertise and significant resources to attempt multiple attack vectors.

Insider Threat

Are network users with trusted access can exploit the systems that protect your most critical assets.

Cybersecurity Today: By the Numbers

In 2018 **financial losses** from **cybercrime** were **$1.3 billion** in the U.S. alone

1 in 131 emails contain **malware**

There are an **estimated 4,000 ransomware attacks** each day, globally

54% of companies say they have experienced **one or more attacks** in the last year

FTI CONSULTING

CYBERSECURITY

FTI Cybersecurity

Risks to ICS/SCADA

ICS/SCADA Risks

- Industrial Internet of Things (IIoT) devices – Air gaps are a thing of the past
- New technologies and third parties with access
- Traditional IT systems now connected to ICS/SCADA – new entry point for hackers
- Network stability versus patch management
- Built without security in mind
- Increase in mobile device usage

ICS/SCADA Cyber Attacks

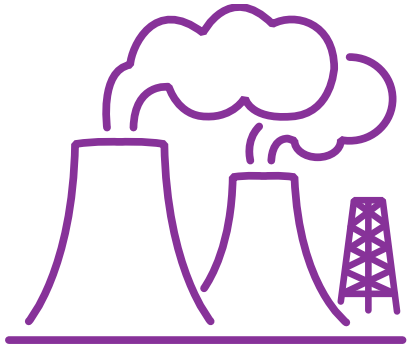
Financial Institution Hack

- One of the largest public sector banks in India
- Hackers gained access to the banks SWIFT system and transferred $170m from the Bank's nostro account in the U.S. to accounts in Cambodia
- FTI Cybersecurity conducted end-to-end incident response identifying chain of events, conducted malware reverse engineering, worked with law enforcement, and helped with remediation

ICS/SCADA Cyber Attacks

Ukraine Power Grid

- Information systems were compromised by hackers at three energy distribution companies
- Electricity supply was disrupted to more than 200,000 people after 30 substations were turned off
- Spear phishing is believed to be how the hackers gained initial access



FTI CONSULTING
CYBERSECURITY

ICS/SCADA Cyber Attacks

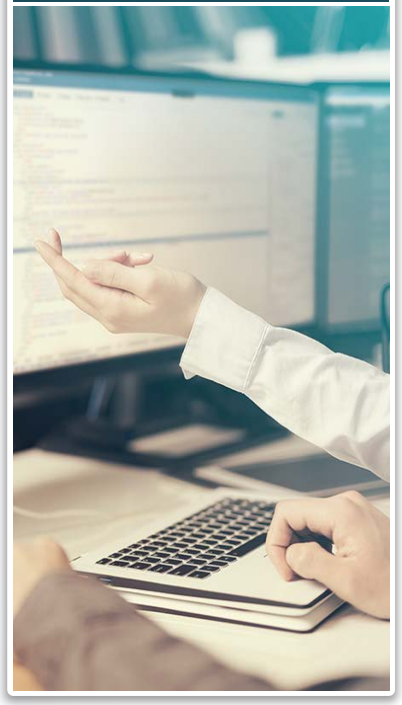
2003 Northeast Blackout

- A power outage resulted in the loss of electricity for more than 50 million people
- The primary cause was due to a software bug at an electric utility in Ohio
- While inadvertent, this demonstrates how the impacts from a targeted attack could be even more severe

FTI Cybersecurity

Core Service Offerings

Our Core Service Offerings

Proactive Services	Incident Response & Investigations	Post-incident/ Remediation Services	Major Complex Investigations	Litigation Support
				

FTI CONSULTING

CYBERSECURITY

Proactive Services

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

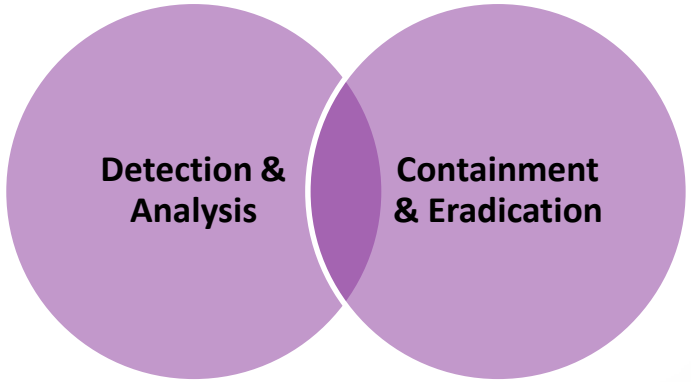
Service Offering	Details / Explanation
Cybersecurity Program Assessment / Posture Review	Scored Assessment of client's Cybersecurity Program to determine overall level of maturity (Policies & Procedures, Technology, Staff, Culture)
Vulnerability Assessments	Technical process to scan for vulnerabilities in client's network (Should be done at least annually, can be component of Posture Review)
Penetration Testing & Red Teaming	Authorized simulated attack on client's system to evaluate security of that system (Can be component of Posture Review)
Threat-Hunting Operations	Proactively searching client's network to identify threats/malicious actors that have already evaded existing security solutions
Crisis Simulation & Table-top Exercises	Live simulated attack to practice and assess readiness
Cybersecurity Compliance Preparedness	Clarification of client compliance landscape and requirements to close gaps and achieve regulatory compliance

FTI CONSULTING
CYBERSECURITY

Incident Response & Investigations

Quick and effective response is critical when it comes to limiting long-term damage. FTI Cybersecurity experts understand that cyber incident response capability must seamlessly integrate across existing mission critical functions, and they have the expertise to respond to all types of threats.

- Respond to all incidents and breaches
- Insider threat investigations
- Ability to deploy anywhere
- Scale to handle complex and largest incidents and breaches
- Proprietary tools for immediate remote deployment



FTI CONSULTING
CYBERSECURITY

Post-incident / Remediation Services

Much the same as the “Proactive” offerings, in “Post-incident activity phase” the incident and incident handling procedures are often analyzed with specific goals in mind – to reduce the probability of similar incident happening again and to improve incident handling procedures

Service Offering	Details / Explanation
Cybersecurity Program Assessment / Posture Review	Scored Assessment of client’s Cybersecurity Program to determine overall level of maturity (Policies & Procedures, Technology, Staff, Culture)
Vulnerability Assessments	Technical process to scan for vulnerabilities in client’s network (Should be done at least annually, can be component of Posture Review)
Penetration Testing & Red Teaming	Authorized simulated attack on client’s system to evaluate security of that system (Can be component of Posture Review)
Threat-Hunting Operations	Proactively searching client’s network to identify threats/malicious actors that have already evaded existing security solutions
Crisis Simulation & Table-top Exercises	Live simulated attack to practice and assess readiness
Cybersecurity Compliance Preparedness	Clarification of client compliance landscape and requirements to close gaps and achieve regulatory compliance

FTI CONSULTING

CYBERSECURITY

Litigation Services

1 Evidence Collection, Handling & Preservation

To gather relevant information within enterprise systems and across diverse data sets.

2 Forensic Analysis

- **Who knew what and when?** Unravel complex cyber incidents and understand intricate relationships between parties
- **Fast action.** Extensive experience and state-of-the-art tools empower FTI to recover, search, and analyze massive amounts of data at the speed demanded by litigation
- **Forensically defensible methodologies.** FTI adheres to court-approved methodologies to preserve evidence for litigation

3 Expert Witness Testimony

Our testifying experts have the experience needed to be effective and persuasive on the stand and in written submissions.

FTI CONSULTING

CYBERSECURITY

FTI Cybersecurity

Additional Service Offerings

Dark Web Research & Analysis

The deep and Dark Web is often where malicious activity is conceived, planned and executed

Breached Domains

IP Theft

Cybercrime

Geopolitical Incidents

FTI CONSULTING

CYBERSECURITY

Dark Web Monitoring

FTI Cybersecurity performs bespoke and tailored investigations into the Deep and Dark Web to complete our investigations.

We search restricted databases and get behind pay-walls. We access registries and filings from jurisdictions around the world. We conduct our investigations in many languages, including Arabic, Farsi, Russian, Chinese and French.

FTI CONSULTING

CYBERSECURITY

Virtual Chief Information Security Officer (vCISO)

FTI Cybersecurity is prepared to act as a company's virtual Chief Information Security Officer. The vCISO is a deployable, managed service that connects top level security experts with organizations that need cybersecurity experience and guidance, with flexibility and scalability that could not otherwise be achieved.

- Information security leadership and guidance
- Security policy and procedure development
- Incident response planning
- Internal audit and penetration testing
- Vulnerability and risk assessments
- Compliance management

FTI CONSULTING

CYBERSECURITY

Cryptocurrency Services

Cryptocurrency is a playground for criminal activity and we offer clients sophisticated investigative services within the cryptocurrency space.

Cryptocurrency Incident Response & Investigations

We deploy advanced tools and techniques to identify and assess evidence of anomalous, suspicious, fraudulent or otherwise illicit activity associated with cryptocurrency assets.

Identification Of Entities / Individuals Behind A Wallet

FTI can analyze transactional relationships and intelligence to identify entities and personas associated with suspect cryptocurrency wallets. Once identified the intelligence is correlated to identify evidence of suspicious, fraudulent or otherwise criminal activity.

Cryptocurrency Services

FTI Cybersecurity's specialized offerings can be leveraged in support of a broad range of litigation and law enforcement matters such as stolen assets, ransomware tracking, anti-money laundering, fraud, trafficking and narcotics investigations.

Cryptocurrency Transaction Tracing, Forensics, & Asset Recovery

Cryptocurrency Anti-Money Laundering

FTI CONSULTING

CYBERSECURITY

Crisis Communications

Effective internal and external communication is imperative during every cybersecurity incident. Our strategic communications teams provide immediate, scalable crisis communications and messaging support around the globe.

Our Communications Experts

- FTI Consulting has a long history of working with clients that have issues preparedness and crises communications needs across industries and around the world.
- Our veteran strategic communications professionals work directly with clients, advisors and FTI Cybersecurity's team to counsel clients in sensitive situations with legal, financial, regulatory and reputational implications.
  - We bring together the right resources to
  - Protect the company's brand, reputation and valuation, and assure customers
  - Demonstrate command of the situation and control the narrative
  - Ensure accurate representation of the facts
  - Engage with stakeholders
  - Reduce legal and political risk
  - Ensure business continuity

When stakes are high, it is imperative to know what to say, how and when to say it, and to whom.

FTI CONSULTING
CYBERSECURITY

Data Privacy Services

Program Development

Data Privacy program build strategy development, program implementation and transformation

Regulatory Enablement

Regulatory gap assessments, policy drafting, compliance process implementation (DPIA, Record of Processing, data mapping), regulatory affairs support (GDPR, HIPAA, CaCPA, etc.)

Privacy Managed Services

Privacy office as a service, DPO as a Service, Crisis Management, On-Call Breach Support.

Privacy Tech Enablement

“Privacy Engineering”, data scanning, automated data mapping, vendor selection support, technology development and implementation.

Privacy Risk Management

Quantitative Privacy and Information Security risk analysis (emerging risk, third party risk, operational risk), control testing, and control tuning.

Deal Support

New venture, M&A privacy due diligence and post-acquisition integration support.

Industry-Specific Solutioning

Technology, Telecom, Media, Financial Services, Healthcare and Life Sciences subject matter experts ready to address nuanced, industry-specific data privacy challenges.

FTI CONSULTING

CYBERSECURITY

FTI Cybersecurity

Select Experience

Financial Data Company
Cyber Breach Crisis Communications

THE CHALLENGE

A major financial data company announced that it had fallen victim to a large-scale cybersecurity breach ultimately affecting millions of U.S. consumers. Following months of public outcry and mounting regulatory pressure, FTI Consulting was brought onboard in early 2018.

OUR INPUT

- FTI Consulting was retained to help the client announce additional, previously unaccounted victims of the 2017 breach.
- FTI developed and executed a comprehensive crisis communications plan alongside the company's communications team, developing messages, conducting media trainings, preparing for Congressional reaction, and providing on-site war room support.
- FTI advocated for a more proactive media outreach effort that demonstrated a greater commitment to transparency and ensured greater accuracy in news reports.

THE RESULT

- FTI has ensured the client's reputation continues to improve following the 2017 cyber incident.
- Helping align the company's multi-pronged communications strategy with broader business objectives and legal obligations, our team has prepared the client's C-Suite leaders to effectively manage several high-profile issues, garnering favorable coverage in top tier news publications around the country. As a result, the client has been able to continue forward in transforming their image as a trusted leader in the financial services sector.

Multi-Billion Dollar Energy-Sector Business Cyber Vulnerabilities

THE CHALLENGE

In connection with an unrelated internal investigation at a multi-billion dollar energy-sector business, FTI Cybersecurity identified several cyber vulnerabilities at the company, as well as employees engaged in suspicious activity.

OUR INPUT

FTI prepared and presented a cybersecurity assessment and a remediation plan to the company's CEO and Board of Directors. In addition, after designing and implementing a cost-effective monitoring program, FTI identified two employees who were actively stealing trade secrets.

THE RESULT

The information developed by FTI's investigation led to successful motions for injunctive relief and to the recovery of the stolen proprietary information. FTI also coordinated successful referrals to federal law enforcement.

FTI CONSULTING

CYBERSECURITY

Large Healthcare Entity
Security Breach

THE CHALLENGE

As security breach resulted in an investigation by the Office of Civil Rights (OCR).

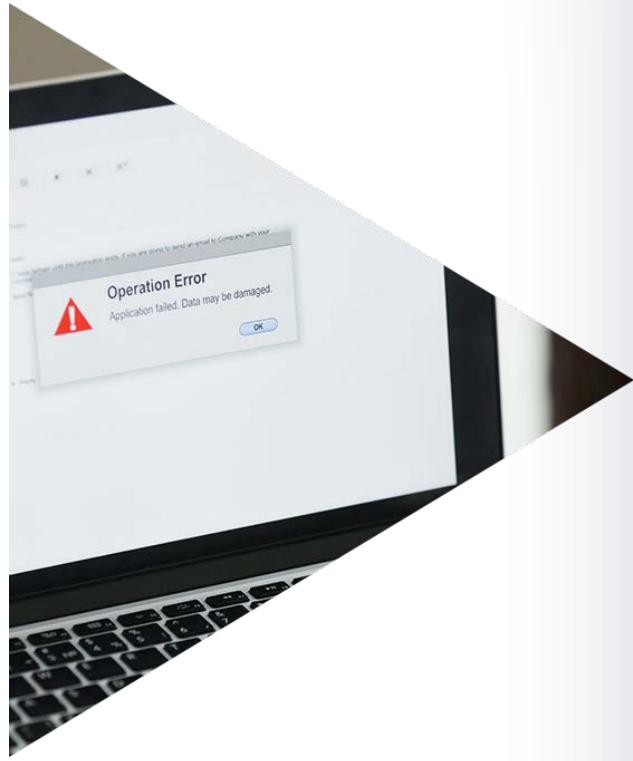
OUR INPUT

FTI Consulting was engaged to help manage breach communication and documentation and to develop a robust privacy and security program to protect against future compliance risk.

THE RESULT

FTI Consulting provided a rapid, initial assessment of the existing privacy and security program, followed by a formal risk assessment report that included specific findings and recommendations. FTI's recommendations allowed our Client to strengthen their privacy and security program to meet the requirements of HIPAA and HITECH.

Global Financial Institution
Internal Investigation of Application Controls



THE CHALLENGE

The Client had experienced a massive financial loss due to a controls/compliance failure in one of their applications, although the root cause of the failure was not initially known. The Client's application ecosystem included several other internally-developed and third-party applications that performed similar functions, but their risk of exposure to another event was unknown.

OUR INPUT

- Reviewed the source code for the Client's application in order to identify the specific factors led to the failure. Demonstrated that the deficiencies still existed even after the Client believed they had properly patched the application.
- Performed a global review of internally-developed and third-party applications in order to assess whether the available controls were adequate to control risk.

THE RESULT

- Identified the programmatic and operational deficiencies that led to the controls failure.
- Presented findings to the Client's board of directors, U.S. regulatory agencies, and credit rating agencies.
- Provided prioritized recommendations in order to mitigate the risk of future failures.

BuzzFeed Defamation Lawsuit

THE CHALLENGE

The “Steele Dossier” was a private intelligence report developed by Christopher Steele, a former head of the Russia desk inside of British Intelligence. The dossier was a collection of memos Steele prepared in 2016 that became part of opposition research efforts during the 2016 U.S. presidential election. BuzzFeed was the first news organization to publish the dossier. However, the company was later sued by a Russian billionaire and technology executive, who was mentioned in the dossier, for alleged defamation. Facing litigation, BuzzFeed retained FTI Cybersecurity to assess whether the plaintiff’s infrastructure was used in the cyber attacks on Democratic Party leadership.

OUR INPUT

Anthony J. Ferrante served as an expert witness in the case. FTI Cybersecurity’s forensic analysis discovered that the plaintiff’s businesses and its affiliated web hosting companies were used as gateways to the Internet for cyber criminals and Russian state-sponsored actors to launch and control large-scale malware campaigns over the past decade without fear of repercussion. For example, FTI Cybersecurity’s analysis determined that “Russian cyber espionage groups” used the plaintiff’s platform to “support malicious spear phishing campaigns against the Democratic Party leadership.”

The FTI Cybersecurity team determined that, based on documentation produced during discovery and deposition transcripts, the plaintiff and associated executives did not appear to actively prevent cyber criminals from using their infrastructure. Minimal, if any, investigations were performed by the plaintiff when their infrastructure was cited in high profile government or private security firm reports.

The investigative findings were reflected in Ferrante’s expert report and described within his testimony.

THE RESULT

In December 2018, BuzzFeed won the case on summary judgment. The ruling judge dismissed the lawsuit deeming BuzzFeed’s publishing of the dossier was “fair and true.” Although our report did not factor into the judge’s analysis, FTI Cybersecurity confirmed that the plaintiff’s infrastructure was used in an attempt to hack the Democratic National Committee.

FTI CONSULTING

CYBERSECURITY

FTI Cybersecurity

How We Can Help

FTI Cybersecurity

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

We help clients of any size address their most critical needs and integrate new solutions atop or alongside pre-existing policies and programs to address cyber threats.

We build a safer future by helping organizations:

Understand their own environments

Harden their defenses

Rapidly and precisely hunt threats

Holistically respond to crises

Recover operations and reputation after an incident

FTI CONSULTING

CYBERSECURITY

FTI Cybersecurity Core Capabilities

FTI Consulting's cybersecurity business is engineered to **synthesize cutting-edge, intelligence-led capabilities around a trusted core of comprehensive offerings.** This enables clients of any size to address their most critical needs and integrate new solutions atop or alongside pre-existing policies and programs

ASSESS & Understand Your Environment

Managing cybersecurity risk begins with developing an organizational understanding of your business environment and its assets. We conduct assessments that inform the development of strategies to manage and mitigate cybersecurity risk to your systems, assets, data, and capabilities.

DEFEND Your Assets and Infrastructure

The deployment of network safeguards is critical. We identify, implement, and manage defensive best practice processes including access control, awareness and training, data protection policies, network maintenance, and deployment of protective technologies. Through these defensive measures, we ensure the delivery of your critical services and operations.

IDENTIFY Threats Rapidly and Proactively

Timely discovery of impacts to your network can be a key factor in minimizing damage. By implementing continuous security monitoring and advanced detection processes on your networks, FTI Consulting experts can detect anomalies and other security-related events rapidly and proactively.

RESPOND to an Incident Holistically

Once you detect a cybersecurity incident, you must act. We provide complete cyber incident response options that include planning, analysis, mitigation, system refinements, and ancillary mission support functions, such as strategic communications and reputation management.

RECOVER Operations Quickly & Sustainably

Restoring capabilities or services that have been impaired is often your top priority when you face a cybersecurity incident. We develop recovery plans that ensure long-term improvement, limit the potential lasting impacts of cyber incidents, and prevent damage from future incidents. With our recovery assistance, you can get back to business as usual, as soon as possible.

FTI CONSULTING

CYBERSECURITY

Why FTI Cybersecurity?

FTI Cybersecurity consists of **300+ dedicated incident response and cybersecurity consultants**, led by those with **decades of experience** at the highest levels of law enforcement, intelligence and global private sector institutions.

Unrivaled depth of experience and integrated expertise

- Integrated team of cybersecurity experts, developers, and data analysts with extensive investigative experience
- Drawing from both government and private sector, FTI's experts routinely tackle large-scale analytic challenges requiring complex custom technical solutions
- FTI regularly constructs and leverages technical platforms to collect, analyze, and correlate data in demanding environments requiring precision and speed

Ability to manage the message should it be needed

- World class crisis communications team can provide immediate and scalable messaging and engagement support should a communication issue arise following FTI's investigation

FTI CONSULTING
CYBERSECURITY

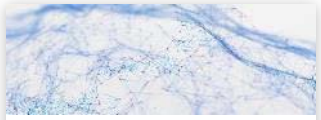
More than Cybersecurity?

Almost every cybersecurity plan, incident response, and investigation brings with it considerations beyond cyber. FTI Consulting is a multinational business advisory, able to support the many issues and challenges associated with cybersecurity.

Global Investigations needed to reveal information, regardless of where it leads.

Forensic Technology to securely collect data anywhere in the world

Forensic Accounting to bring understanding to financial information



Data & Analytics to process and analyze vast amounts of data

Crisis Communications to formulate internal and external communications in the wake of a cyber incident

Anti-Money Laundering professionals, themselves former regulators and Big-4 auditors, expert in compliance for financial institutions

Unmatched Global Reach

FTI CONSULTING

CYBERSECURITY

Ron Yearwood
Senior Managing Director
+1 415 283 4200
ron.yearwood@fticonsulting.com

About FTI Consulting

FTI Consulting, Inc. is a global business advisory firm dedicated to helping organizations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. With more than 4,600 employees located in 29 countries, FTI Consulting professionals work closely with clients to anticipate, illuminate and overcome complex business challenges and make the most of opportunities.