Insights: Top Disputes & Investigations

Cybersecurity

EXPERTS WITH IMPACT™

FTI CONSULTING

Cybersecurity

Cybercrime is growing rapidly as a result of the global pandemic: cyber-criminals prey on individuals and companies who may be less guarded as they cope with this global pandemic.

FTI Cybersecurity has some of the industry's most prominent experts on cybersecurity, digital forensics and remediation. The team has been engaged in several high-profile cases and disputes involving cybercrime and malware that affect all types of companies and organizations. In this section, of our **2020 Insights: Top Disputes & Investigations**, we highlight our work helping clients resolve disputes on major Cybersecurity projects.

BuzzFeed Wins Dossier Defamation Lawsuit

The "Steele Dossier," also commonly known as the "Trump Dossier," was a private intelligence report developed by Christopher Steele, a former head of the Russia desk for British Intelligence. The dossier was a collection of memos Steele prepared in 2016 that became part of political 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 statements in the dossier were valid – that the Plaintiff's infrastructure was used in the cyberattacks on Democratic Party leadership.

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.

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.

Subject Matter Experts

Anthony J. Ferrante
Senior Managing Director

Katie Donnelly
Managing Director

Joe Knight
Managing Director

Interim vCISO Steps in After Breach

One of the largest distributors of Caterpillar equipment in the Middle East and North Africa fell victim to a business email compromise and cybersecurity breach that resulted in over $10 million in wire transfer fraud.

In response, we deployed a dedicated expert to immediately act as the interim virtual Chief Information Security Officer (vCISO). The vCISO helped build the Company's cybersecurity strategy and align cybersecurity policies and practices with industry standards. We also implemented an incident response plan and introduced various tools, procedures, and capabilities. We seamlessly transitioned the work to an in-house leader by onboarding a new, dedicated CISO. Additionally, we trained new staff on proper cybersecurity policies and procedures.

With a new in-house CISO, plans and procedures in place, the Company is now able to better protect itself from risk exposure from the cyber threat landscape.

Subject Matter Experts

Anthony J. Ferrante
Senior Managing Director

Ron Yearwood
Senior Managing Director

Praveen Madhavankutty
Managing Director

David Dunn
Managing Director

Dark Web Research and Breach Recovery for a Major Online Fashion Retailer

A major online fashion retailer that ships to more than 80 countries experienced a security breach that affected more than six million customers. The sophisticated cyber attack on the company's computer network initially went undetected, allowing the attackers to move freely through the company's systems for months.

FTI Cybersecurity was hired to provide intelligence services to identify whether any customer data from the breach was posted on the dark web and if so, what data was exposed. Using FTI Cybersecurity's proprietary dark web threat intelligence tool, our team was able to quickly determine that customer data was posted in two locations, auctioned for sale, and ultimately exchanged between criminal actors. FTI Cybersecurity also verified the exact number of affected customers and determined that the stolen information posted and sold on the dark web was limited to email addresses and encrypted passwords.

Our team was able to minimize the distribution of the data that was posted on public and semi-public dark web forums, but the work did not stop there. Partnering with FTI's Strategic Communications experts, an inbound call center was up and running in less than a week with scripts in multiple languages developed for servicing affected customers.

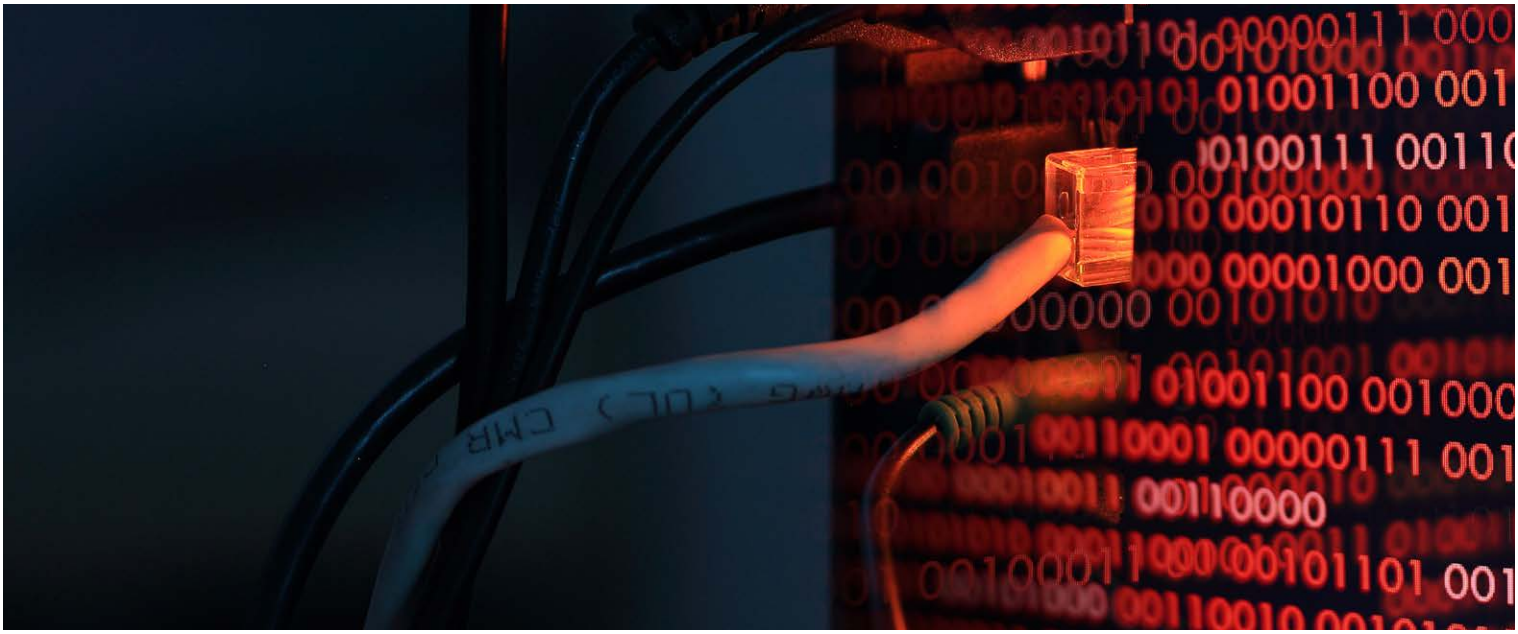
Subject Matter Experts

Jordan Rae Kelly
Senior Managing Director

Ron Yearwood
Senior Managing Director

Myron Marlin
Senior Managing Director

Elizabeth Cholis
Managing Director



Ransomware Response for a Provider of Billing and Finance Software

At about 3 a.m. on a Saturday morning, FTI Cybersecurity's client (a billing and finance software company) began receiving critical alerts related to its network. The company was hit by a sophisticated ransomware attack that encrypted all of its servers and halted critical business operations, leaving it in a race against the clock to save the company.

Within hours of approval, FTI Cybersecurity's team boarded a flight to the company's office. Immediately upon arrival, the team started hardware imaging and analysis to determine the strain of ransomware and available options. Given the risks, FTI Cybersecurity established the deadline for defeating the ransomware as 3 a.m. Tuesday morning (72 hours from attack), when negotiations with the malicious actor would begin. Unfortunately, although the ransomware was quickly identified, there was no known way to quickly decrypt the files, so negotiations began with the malicious actor. Although the client was prepared to pay the full ransom demand, FTI brought in a Strategic Communications team to craft a communications plan to negotiate a lower fee.

Our team successfully negotiated a reduced ransom, resulting in significant savings for the client. The FTI teams 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.

Subject Matter Experts

Anthony J. Ferrante
Senior Managing Director

Jordan Rae Kelly
Senior Managing Director

Brian Kennedy
Senior Managing Director

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™