Business Email Compromise Services

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

Business Email Compromise (BEC) is characterized by the use of email as a vector by which threat actors attempt to cause their victim to provide payment or sensitive information to the threat actor under the pretense of legitimate business practices. Threat actors continually evolve their tactics, incorporating Email Account Compromise, creating increasingly realistic emails and circumventing conventional controls. In 2023, the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) received 21,489 BEC complaints, for a combined loss of more than $2.9 billion.

FTI Cybersecurity has deep experience assisting organizations in the prevention of, and response to, BEC attacks.

BEC Prevention

Program assessments & MFA

- Perform analysis to identify compromises to email servers and if alterations were made
- Implement multifactor authentication (MFA) wherever possible to add an additional layer of protection against compromised credentials

Phishing awareness training

- Comprehensive reporting on campaign results, providing trends on caught employees
- Test phishing emails are tailored using results from the latest campaigns
- Custom-built phishing emails for C-suite demonstrations

BEC Response

Once a BEC incident is identified, FTI Cybersecurity combines the resources and tools necessary to determine the scope, impact, and appropriate response. Through digital forensic analysis, we proactively identify and block known indicators of compromise to mitigate cyber risk and eliminate the threat. Our experts have extensive technical and investigative experience and strong connections with law enforcement agencies, allowing for thorough investigations and assistance in the recovery of stolen assets.

CASE STUDY

BEC IMPACTS MAJOR AIRPORT TERMINAL

SITUATION

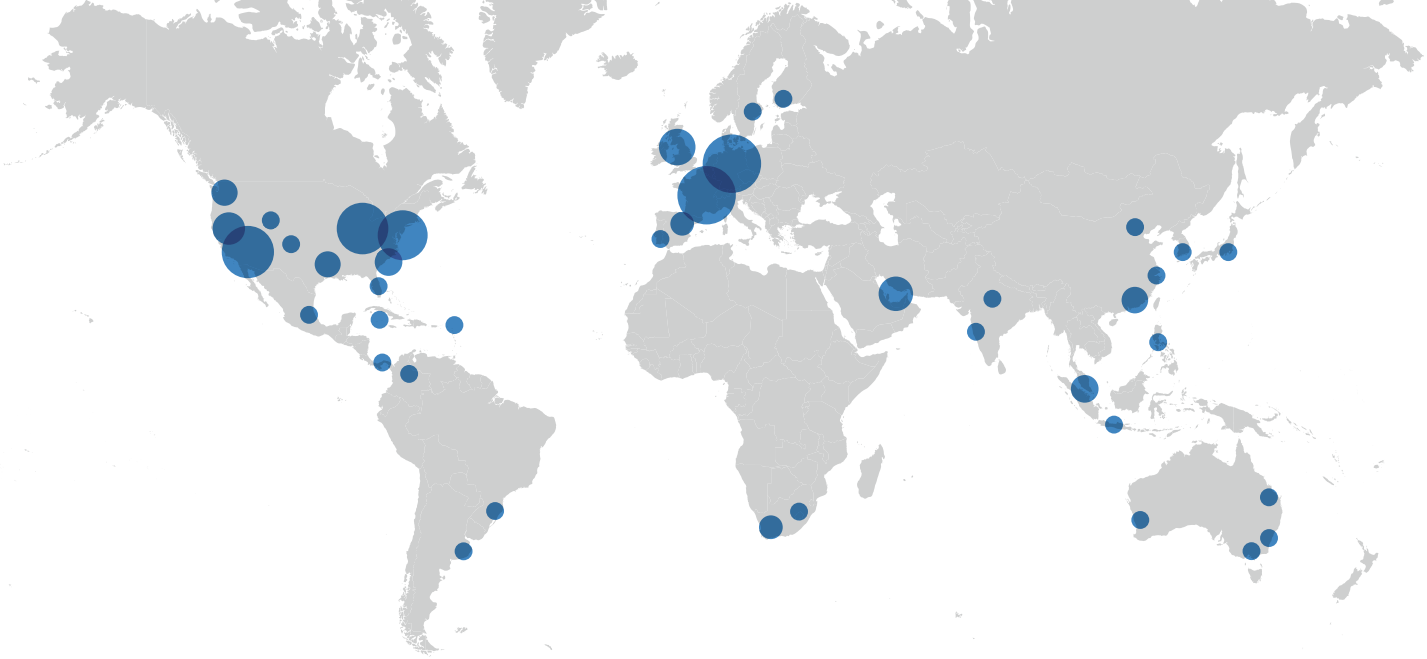
The client, an airport terminal, wired a payment of $47 million dollars to the incorrect account as the result of a BEC attack. The client identified spoofed domains, and retained FTI Cybersecurity to investigate how the BEC occurred, track the flow of money from the account, and assist with the recovery of funds.

OUR ROLE

We worked with the client to review Microsoft 365 (M365) activity and the spoofed emails. Our experts examined the dark web for potential leaked credentials or client materials, and identified additional accounts that were compromised. Through existing connections, we coordinated with law enforcement and financial institutions to track the movement of stolen funds.

OUR IMPACT

After our review and analysis, we provided recommendations to harden and secure the client's M365 environment. We identified the point of compromise and drafted a strategy to remove threat actor access from the environment. Our coordination with law enforcement helped track and return nearly all $47 million.



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

1982

Year Founded,
Publicly traded **NYSE:FCN**,
$7.7B Equity Market Cap*

38/50

Advisor to 38 of the world's top 50 bank holding companies

8,000+

Employees Worldwide

64/100

Advisor to 64 of the top 100 Private Equity International ("PEI 300") firm

98/100

Advisor to 98 of the world's top 100 law firms

83/100

83 of Fortune 100 corporations are clients

**Number of total shares outstanding as of April 18, 2024, by the closing price per share on April 25, 2024.*

HAVE AN INCIDENT?
#FTICYBERSECURITY-RESPONSE
@fticonsulting.com

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

08062024 | VN03592-v05 Business Email Compromise