

# Cybersecurity

## Ransomware Response Services

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

When ransomware strikes, you have little time to decide what to do – payments for some variants increase each day you wait. FTI Cybersecurity can help implement processes to prevent an incident, provide immediate response to a successful attack, and assist with the recovery process. This includes investigation, decryption, and even negotiation with the malicious actor if needed.

Although only a fraction of ransomware incursions is reported, cyber criminals ask for \$5,000 to upwards of \$25 million in cryptocurrency payment to send a cure. Regardless of the dollar value of the requested ransom, the financial cost from recovery efforts due to inadequate security protections can often far exceed the ransom. Effective planning will prevent many ransomware attacks and allow you to recover quickly if you are impacted.

### How FTI Cybersecurity can help:

1. Respond to incidents immediately and serve as first responders
2. Collect artifacts to discover active infections and identify entry points
3. Conduct analysis to determine scope of infection and all impacted systems
4. Initiate recovery operations to eradicate infection
5. Provide crisis management and strategic communications
6. Rebuild infrastructure and implement best practices to prevent repeat attacks
7. Identify techniques, tactics, and procedures associated with threat actors and coordinate with law enforcement, if appropriate

### How is data unlocked?

Either by decrypting the code, which can be difficult, laborious, and many lack this capability internally, or by paying the ransom, which can be costly, is usually done with cryptocurrencies, and encourages more ransom attempts without addressing the underlying issue.

### How damaging can an attack be?

We're currently seeing a ransomware strain, Snake or EKANS, aggressively targeting a range of organizations, with an uptick in activity since the COVID-19 crisis began. In 2017 the WannaCry ransomware attack is thought to have cost \$8 billion worldwide.

### CASE STUDY: E-COMMERCE BILLING & FINANCE PLATFORM

#### THE CHALLENGE

An e-commerce billing platform suffered a ransomware attack. Weak customer credentials led to a highly successful, laterally moving attack that was able to successfully encrypt servers in a matter of hours. The attack paralyzed operations and prevented the company's clients from processing bills and transactions. The company was in a race against the clock.

#### OUR INPUT

We assembled a cross-segment team to deploy to the client site immediately. Our experts quickly determined the ransomware to be a new strain of Bitpaymer, FriedEx.

#### OUR IMPACT

FTI Cybersecurity alongside our technology and strategic communication experts were successful at negotiating with the malicious actor, saving the client hundreds of thousands of dollars and preventing significant customer and revenue loss.



## 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

No other firm in the space has a crisis communications practice

Integration of FTI Consulting's expertise across the platform

# 29

Countries

# 1982

Year Founded

# 6,400+

Employees

# NYSE:FCN

Publicly traded

# 8/10

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

# 96/100

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

# \$4.8B

Equity Market Capitalization\*

# 55

55 of Fortune Global 100 corporations are clients

\*Number of total shares outstanding as of April 22, 2021, times the closing share price as of April 29, 2021.

#### ANTHONY J. FERRANTE

Global Head of Cybersecurity  
Senior Managing Director  
+1 202 312 9165  
[ajf@fticonsulting.com](mailto:ajf@fticonsulting.com)

#### JORDAN RAE KELLY

Head of Cybersecurity, Americas  
Senior Managing Director  
+1 202 312 9140  
[jordan.kelly@fticonsulting.com](mailto:jordan.kelly@fticonsulting.com)

#### KYUNG KIM

Head of Cybersecurity, APAC  
Senior Managing Director  
+82 2 2190 3727  
[kyung.kim@fticonsulting.com](mailto:kyung.kim@fticonsulting.com)

#### DAVE HARVEY

Managing Director, EMEA  
United Kingdom  
+44 207 632 5147  
[dave.harvey@fticonsulting.com](mailto:dave.harvey@fticonsulting.com)

#### KEVIN WONG

Managing Director, EMEA  
Middle East  
+971 54 586 7142  
[kevin.wong@fticonsulting.com](mailto:kevin.wong@fticonsulting.com)

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. ©2021 FTI Consulting, Inc. All rights reserved. [www.fticonsulting.com](http://www.fticonsulting.com)

06142021 | VN01465-v04

