FTI CONSULTING | CYBERSECURITY

# FTI CYBERSECURITY BRIEFING BOOK

MARCH 2019

FTI CYBERSECURITY MONTHLY NEWSLETTER

## Welcome to the FTI Cybersecurity Briefing Book

FIRST ISSUE

The FTI Cybersecurity Briefing Book is your monthly window into the latest news from around the industry and highlights from our global practice. The Briefing Book provides team and service offering updates, as well as trends that we are identifying that may affect your organization. We also highlight case studies that show the depth, scope, and nature of work that we do for clients.

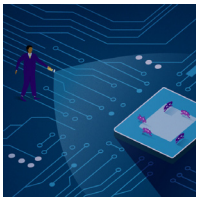
### About FTI Cybersecurity

FTI Cybersecurity's structure and capabilities are engineered to synthesize cutting-edge intelligence-led cybersecurity practices around a trusted core of comprehensive offerings. Our team enables clients of any size to address their most critical needs and integrate new solutions atop or alongside any preexisting policies and programs.

IN THIS ISSUE...



## Recent Thought Leadership



*Cyber Criminals Are Exploiting the Dark Web. Here's Why You Should Too*

The ominous-sounding "dark web" is often associated with criminal activity, and there is no denying that it is used as a platform for illicit purposes. But it also has features that can be used to your advantage, specifically concerning cybersecurity.

In this *FTI Journal* article, Managing Director David Dunn details how cyber criminals are exploiting the dark web and why you should too.

Read more about what the dark web is and how to leverage it for proactive cybersecurity defense.


*10 Corporate Cybersecurity Predictions*

In the fast-moving world of cybersecurity, predicting the full threat landscape is near impossible. But it is possible to extrapolate major risks in the coming months based on trends and events of last year.

In this article featured in *Corporate Compliance Insights*, Anthony J. Ferrante, Senior Managing Director and Global Head of FTI Cybersecurity, outlines what you must be aware of to be prepared.

Read what you need to know for 2019 – and beyond.

SERVICE SPOTLIGHT

# Preparedness Planning: Testing an Organization's Cyber Readiness

In today's increasingly connected world, all organizations are at risk from cyber-related threats. A cyber incident can both cripple organizations and permanently damage the reputation of your business.

## What We Offer

FTI Cybersecurity offers custom crisis exercises and evaluations designed to test and improve an organization's incident response capabilities.

Our Preparedness Planning services focus on developing best practice crisis management skills and knowledge. We will improve your organization's ability to address the various phases of an emerging crisis, discussing options and making consequential decisions at each juncture.

## Create Real-World Scenarios

The aim is to replicate the operational and communications challenges of a cyber incident through realistic pivot points and role play. Using real-world scenarios and simulations, we help you understand your threat profile, prepare a response plan, enumerate your potential vulnerabilities, and harden your defenses.

## Who Should Attend

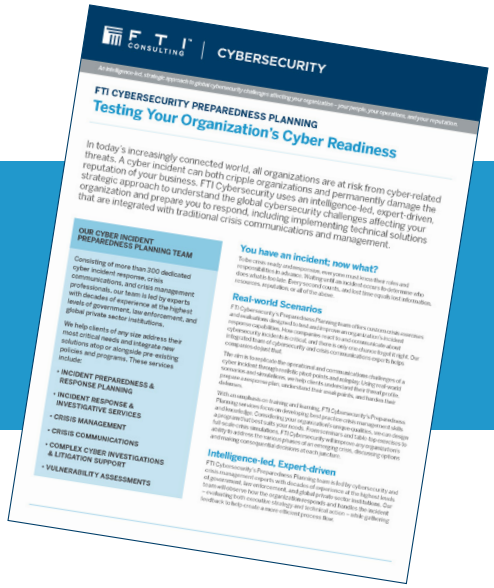
This offering is geared towards C-Suite, board members, senior management, chief risk officers, general counsel, business continuity planning teams, technical leaders, communications, media & public affairs teams, and customer service teams.

## Benefits Include

- Highlight strengths and identify vulnerabilities in your organization's existing crisis processes, structures, and skills
- Test your organization's ability to respond to regulatory requirements in proper timeframes
- Test your organization's process to engage appropriately with law enforcement
- Receive in-depth feedback and analysis together with recommendations for optimizing your crisis policies and processes
- Test and learn best practices for engaging with media, employees, customers, vendors, partners, regulators, and other key stakeholders

If you would like to learn more, please email #Cybersecurity-Marketing@fticonsulting.com

**Download Service Sheet**


F T I CONSULTING | CYBERSECURITY

FTI CYBERSECURITY PREPAREDNESS PLANNING

Testing Your Organization's Cyber Readiness

In today's increasingly connected world, all organizations are at risk from cyber-related threats. A cyber incident can both cripple organizations and permanently damage the reputation of your business. FTI Cybersecurity uses an intelligence-led, expert-driven, strategic approach to understand the global cybersecurity challenges affecting your organization and prepare you to respond, including implementing technical solutions that are integrated with traditional crisis communications and management.

OUR CYBER INCIDENT PREPAREDNESS PLANNING TEAM

Consisting of more than 200 dedicated cyber incident response, crisis communications, and crisis management professionals, our team is led by experts with decades of experience at the highest levels of government, law enforcement, and global private sector institutions.

We help clients of any size address their most critical needs and integrate new solutions atop or alongside pre-existing policies and programs. These services include:

- INCIDENT PREPAREDNESS & RESPONSE PLANNING
- INCIDENT RESPONSE & INVESTIGATIVE SERVICES
- CRISIS MANAGEMENT
- CRISIS COMMUNICATIONS
- COMPLEX CYBER INVESTIGATIONS & LITIGATION SUPPORT
- VULNERABILITY ASSESSMENTS

You have an incident; now what?

Real-world Scenarios

Intelligence-led, Expert-driven

WHAT'S TRENDING

## Banking Trojans Going Mobile

Trojan attacks have decreased over the years, but new banking versions of this infiltration technique have recently emerged. The objective is to create a backdoor for data theft purposes, either to compromise bank accounts or for identity theft. Regardless of the intent, the end goal is the same – to fraudulently obtain money. Several financial institutions in Spain were recently attacked via BackSwap, which involves injecting code into the user's browser in order to intercept and monitor communications, specific to banking/financial information.

Not only is the use of banking trojans on the rise, but it is evolving and moving towards targeting mobile devices. In McAfee's 2018 Mobile Threat Report, they noted a "77 percent increase in banking trojans and predicted that this type of exploitation would continue to grow," which it unfortunately did. From June to September 2018, they "detected 2x increase in banking trojans, with the Banker family of malware showing the strongest growth, followed by a further 75 percent spike in December."

## Phishing Isn't Just Email Anymore

Emerging cyber threats associated with IoT and artificial intelligence are hot topics, but simpler threats, like those stemming from phishing attacks, should not be overlooked. Phishing is usually linked with email as the attack method, but malicious actors are now using an array of platforms to achieve their goals. Fake websites that look legitimate – complete with the padlock icon – posts on social media, online ads, browser extensions, and messaging services are all new frontiers that attackers are leveraging.

Employee awareness is key to spotting and reporting phishing, but it's likely that training is focused on email as the attack vector. This needs to be expanded to include additional avenues, so that employees know threats exist outside of their inbox. It's easy to focus on more interesting threats, but considering that "93 percent of confirmed data breaches" involved phishing, this is a threat that all companies – and individuals – need to seriously consider (2019 Verizon Data Breach Investigations Report).

**How FTI Cybersecurity Can Help**

Every exploit has the potential to affect an organization's integrity and could lead to lost revenues or loss of confidence with the customer. FTI Cybersecurity builds a safer future by helping organizations understand their own environments, harden their defenses, rapidly and precisely hunt threats, holistically respond to crises, and sustainably recover their operations and reputation after an incident.

IN CASE YOU MISSED IT

# FTI Cybersecurity Expands Its Practice with the Appointment of Jordan Rae Kelly as Senior Managing Director

Jordan Rae Kelly, former Director for Cyber Incident Response at the U.S. National Security Council and Chief of Staff for the Federal Bureau of Investigation's Cyber Division, has joined the firm's Cybersecurity practice as a Senior Managing Director.

Ms. Kelly, who is based in Washington, DC, most recently served as a senior cybersecurity policy advisor to the Trump administration. In this role, she was responsible for coordinating national cyber incident response and managing zero-day exploits. She also co-authored and contributed to the National Cyber Strategy released in September 2018 and led the U.S. government policy process on encryption.

Click to read the press release

*"Jordan is an established leader with extensive experience working across U.S. government agencies to implement policies and protect our nation from cyber threats."* – Anthony J. Ferrante, Global Head of Cybersecurity

**Jordan Rae Kelly**
Senior Managing Director
Washington, DC
jordan.kelly@fticonsulting.com

## In the Media

*Washington Life Magazine's Tech 25 List*
Anthony J. Ferrante is featured in *Washington Life*'s annual Tech 25 list among other local entrepreneurs making noteworthy contributions to the technology sector. Click to read the feature.

*North Korean-backed Bank Hacking on the Rise, US Officials Say*
Anthony J. Ferrante commented on the North Koreans' rise to become the world's best digital bank robbers in a CNN article. Click to read the article.

*Tech Firm in Steele Dossier May Have Been Used by Russian Spies*
*The New York Times* mentions Anthony J. Ferrante's expert report and FTI Consulting's work on the BuzzFeed dossier case. Click to read the article.


*Tech Company in Steele Dossier May Have Been Used to Support DNC Hack*
*BuzzFeed News* reviews the findings of Anthony J. Ferrante's expert report in regard to the BuzzFeed dossier case. Click to read the article.

*Expert in Trump Dossier Trial Says Tech Firm's Services Were Used in Hack of Democrats*
*McClatchy* reviews the findings of Anthony J. Ferrante's expert report in regard to the BuzzFeed dossier case. Click to read the article.

A LOOK BACK & AHEAD

## Presentations from Recent Events


*RSA Conference 2019*
**March 4 - 8 | San Francisco**

Anthony J. Ferrante spoke in a session titled, "AI: Hacking Without Humans, How Can Human Brains Be Hacked?" and in a session titled "Investigating IoT Crime: The Value of IoT Crime Classification," which was moderated by Jordan Rae Kelly.

## Upcoming Events & Speaking Engagements

*Incident Response Forum 2019*
**April 10 | Washington, DC**

Incident Response has quickly become the fastest growing practice area at law firms and consulting firms. During this single-day event, Jordan Rae Kelly will moderate the afternoon keynote with Assistant Attorney General for the National Security Division, U.S. Department of Justice, John Demers. Click to learn more.

*Patent Disputes Forum 2019*
**April 17 | Menlo Park**

Anthony J. Ferrante will participate in a panel titled, "Adapting Cybersecurity Tactics for the Interconnected World." Click to learn more.

*SPARK CXO Leadership Series*
**April 25 | Napa**

Spark is a private, invitation-only event series created for extraordinary leaders in technology and business. Anthony J. Ferrante will participate in a panel discussion on data cybersecurity and will deliver a visionary address on the global cybersecurity landscape. Click to learn more.

*Regional Meeting of the Compliance Governance and Oversight Council (CGOC)*
**April 25 | New York**

The CGOC regional meeting is a one-day event designed exclusively for IT, legal, privacy, and security experts who need to understand the impact of the evolving compliance and security environment on data management. Click to learn more.

*CPR-FTI Cybersecurity "Cybersecurity in ADR Training"*
**April | Webinar Series**

FTI Cybersecurity has partnered with the International Institute for Conflict Prevention and Resolution (CPR) to offer an exclusive new benefit for arbitrators and mediators. Click to learn more.

To learn more about FTI Cybersecurity, please visit: **www.fticybersecurity.com**

Follow us on Twitter! **@FTICyber**