FTI CYBERSECURITY BRIEFING BOOK

FTI CYBERSECURITY MONTHLY NEWSLETTER

MAY 2019

IN THIS ISSUE...

SERVICE SPOTLIGHT
CYBERSECURITY PROACTIVE SERVICES

ABOUT OUR OFFERING

WHY PROACTIVE SERVICES ARE IMPORTANT

Building a robust security posture is the best way to prevent a breach from occurring. You cannot control if you will be the victim of a cyber attack or not, but you can control how to respond to one. Effective and tailored incident prevention measures can help preserve your corporate reputation, operations, and financial standing. Waiting until an incident has occurred to act is too late.

WHY FTI CYBERSECURITY

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

Our experts 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.

WHAT WE OFFER

- Cybersecurity Program Assessments
- Penetration Testing
- Threat-Hunting Operations
- Vulnerability Assessments
- Red Teaming
- Policies, Procedures, and Staff Gap Analysis & Design
- Cybersecurity Compliance
- Incident Preparedness & Response Planning
- Crisis Simulation & Table-Top Exercises
- Employee Training

If you would like to learn more, please email #FTICybersecurity.

Download Service Sheet

WHAT'S TRENDING
QUANTUM DECRYPTION AND SIM HIJACKING

A POST-QUANTUM WORLD

Today, we commonly hear "artificial intelligence" and the "Internet of Things" in connection with the latest technology trends. But what about quantum computing? "Current computers manipulate individual bits, which store information as binary 0 and 1 states. Quantum computers leverage quantum mechanical phenomena to manipulate information" (IBM). Organizations that are in the medical and financial sectors, dependent on supply chain logistics, or leveraging artificial intelligence will see powerful changes in efficiency, innovation, and analytic capabilities. Yet quantum computing will bring enormous risk to encrypted data. It will have the ability to "break today's strongest asymmetric-key encryption in milliseconds or minutes" (CSO). This new way of computing may not be widely adopted tomorrow, but quantum computers are on the horizon. Organizations will face the challenge of planning for the future and considering how to protect personally identifiable information for the lifetime of the person it relates to, and to follow new encryption standards will require planning, resources, and executive buy-in.

HOW VALUABLE IS YOUR PHONE NUMBER?

An indictment was filed last month against several people who allegedly used SIM hijacking to steal cryptocurrency valued at more than $2.4 million (Cyberscoop). SIM hijacking, also known as SIM swapping, is a growing threat where hackers deceptively transfer the target's phone number from one device to another. Often leveraging social engineering, the hackers will pose as the target and request that the phone number is ported to a new SIM card – one that the hacker already owns. Alternatively, hackers will sometimes work directly with employees at carrier companies, bribing them for assistance in the SIM swap. Once the SIM is updated, the malicious actor can gain access to the victim's accounts, change passwords, and bypass security measures like two-factor authentication. While it's difficult to quantify how often SIM hijacking occurs each year, it is an emerging threat to not only individuals but to companies who may be compromised through their employees, or carrier companies, who may be accused of being liable for these attacks.

HOW FTI CYBERSECURITY CAN HELP

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

IN THE MEDIA

HOW NEST, DESIGNED TO KEEP INTRUDERS OUT OF PEOPLE'S HOMES, EFFECTIVELY ALLOWED HACKERS TO GET IN

Anthony J. Ferrante was quoted in this Washington Post article about the ease in which hackers can break into Nest devices through credential stuffing and the security challenges the company faces in light of these hacks. Click to read the article.

THE NSA KNOWS ITS WEAPONS MAY ONE DAY BE USED BY ITS TARGETS

In this Cyberscoop article, Jordan Rae Kelly comments on the Vulnerabilities Equities Process (VEP) and how government agencies decide to use capabilities against targets abroad despite the risk that they may eventually be used by an adversary. Click to read the article.

A LOOK BACK & AHEAD

RECENT SPEAKING ENGAGEMENTS

KING & SPALDING CYBERSECURITY & PRIVACY SUMMIT

May 1 | Atlanta, GA

FTI Cybersecurity's Jordan Rae Kelly participated in a panel on economic espionage, and Strategic Communications' Meredith Griffanti participated in a panel covering the public relations issues that arise with cyber incidents.

SECURITIES ENFORCEMENT FORUM WEST

May 9 | East Palo Alto, CA

At this securities enforcement conference, Anthony J. Ferrante participated in a panel, "Cybersecurity Disclosure and Enforcement: Will the SEC Drop the Hammer in 2019?" with participants from Cooley, the SEC, and Morrison & Foerster.

FTI CONSULTING & REED SMITH SIMULATED CYBER ATTACK

May 21 | London, UK

FTI Cybersecurity and Strategic Communications co-hosted a simulated data breach breakfast program with Reed Smith for corporate senior executives and legal and compliance professionals.

UPCOMING EVENTS & SPEAKING ENGAGEMENTS

SECURITY & RISK LEADERSHIP ACADEMY

June 5 | Skytop, PA

At a three-day course hosted by Gavin de Becker & Associates, Anthony J. Ferrante will discuss with fellow security leaders the current cybersecurity threats we face, how to mitigate cybersecurity risk within an organization, and the return on cybersecurity investments.

A LOOK BACK & AHEAD (CONTINUED)

LEGAL INNOVATION & TECH FESTIVAL
June 12 | Sydney, Australia

FTI Technology's Chris Hatfield will present on drone forensics and emerging technologies at this two-day, four conference event. Click to learn more.

IOT SECURITY SUMMIT
June 12 | Webinar

Jordan Rae Kelly will discuss the IoT threats facing the healthcare sector, as well as strategies for managing and mitigating cyber risks. Click to learn more.

IG3 MID-ATLANTIC CONFERENCE
June 26 | Washington, DC

FTI Cybersecurity will participate in an incident response panel that will discuss how and why timely and effective breach reporting matters and how to discuss a big cyber breach in the manner best to minimize reputational harm. Click to learn more.

Have you registered for ICCS 2019? Click to learn more.

FTI Cybersecurity is proud to be a gold sponsor of the 8th International Conference on Cyber Security.
July 22 - 25 | New York, NY

FOR MORE INFORMATION

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

Follow us on Twitter!
@FTICyber

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.