FTI CYBERSECURITY BRIEFING BOOK

FTI CYBERSECURITY MONTHLY NEWSLETTER

JANUARY 2021

IN THIS ISSUE...

WHAT'S TRENDING
THREATS IN THE CLOUD

Today, companies' critical data is often entrusted to cloud service providers in order to save the organization time and money. However, cloud migration is happening at a speed that often surpasses the security controls required to secure an organization's most sensitive data.

Digital transformation is a huge undertaking that can leave a company vulnerable to cybersecurity incidents. The primary weakness is not within the cloud infrastructure, but rather the human component. The migration process leaves so many opportunities for errors as IT teams configure access, storage, security, and monitoring controls. In an Analysis Report published by the Cybersecurity and Infrastructure Security Agency (CISA), it is reported that threat actors are using "a variety of tactics and techniques, including phishing, brute force login attempts, and possibly a 'pass -the-cookie' attack, to attempt to exploit weaknesses in the victim organization's cloud security practices." The current remote working environment and use of shadow IT contributed to the prevalence of these attacks as they revealed weaknesses in the cloud environment and security practices.

To strengthen cloud security, organizations should implement basic best practices, such as multi-factor authentication, and policies that limit user access and prohibit the use of personal devices. CISA recommends that organizations take the following steps:

- Implement conditional access policies based upon your organization's needs.
- Establish a baseline for normal network activity within your environment.
- Have a mitigation plan or procedures in place; understand when, how, and why to reset passwords and to revoke session tokens.
- Consider restricting users from forwarding emails to accounts outside of your domain.
- Focus on awareness and training. Make employees aware of the threats and how they are delivered.
- Ensure existing built-in filtering and detection products are enabled.
- Establish blame-free employee reporting and ensure that employees know who to contact when they see suspicious activity or when they believe they have been a victim of a cyber attack.

HOW FTI CYBERSECURITY CAN HELP

We develop a customized roadmap for cloud adoption, optimize policies, processes, and programs needed for developing cloud solutions, and assess client's data management lifecycle and compliance posture to implement effective security controls.

SERVICE SPOTLIGHT
CYBER READINESS SERVICES

All organizations are vulnerable to cybersecurity risk. Being sufficiently prepared relies on several factors including specific regulation demands, nature of business conducted, type and amount of information stored, and scale and scope of the organization's footprint. FTI Cybersecurity works with your team to evaluate your specific needs to tailor solutions that enhance security and readiness to defend against the unique cybersecurity risks facing your organization.

READINESS SERVICES

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.

- Cybersecurity Program Assessment
- Penetration Testing
- Threat-hunting Operations
- Vulnerability Assessments
- Red Teaming
- Policies, Procedures, Staff Gap Analysis & Design
- Cybersecurity Compliance
- Crisis Simulation & Table-top Exercises
- Dark Web Intelligence Monitoring
- Third Party Audit & Assessments

CASE STUDY
Cybersecurity Dashboard for a Technology Company

Situation
A technology company needed assistance with their risk management processes, including how to explain existing issues to executive.

Our Role
Our team was hired to analyze key performance indicators, evaluate their reporting structure, and help articulate their cybersecurity risk to senior leadership.

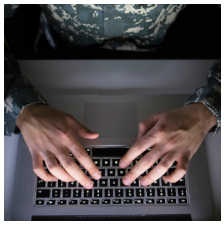
Our Impact
Our experts helped develop a monthly dashboard designed to address deficiencies with rigor and urgency, and to hold relevant teams accountable for progress. The dashboard summarized the organizational risk and remediation plans aligned by four security functions within the company.

DOWNLOAD HERE

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

IN CASE YOU MISSED IT

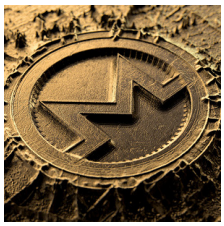
ALERT



UPDATE: SUNBURST/SOLARIGATE ACTIONABLE GUIDANCE

FTI Cybersecurity continues to closely monitor recent developments and IOC source lists. Please refer to the updated guidance for our most recent intelligence and recommendations. To further support the community, we are offering **free impact assessments** to organizations suspecting compromise or increased risk. Click to access.

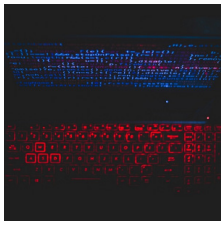
IN THE MEDIA



NEW GOLANG-BASED WORM TARGETS SERVERS TO MINE MONERO

Head of Cybersecurity for the APAC region Kyung Kim comments on how the Golang malware works and its use among threat actors in this *InfoRisk Today* article. Click to read.

THOUGHT LEADERSHIP



A DISTURBING TREND – ROAD TO A CYBER DARK AGE

Global Head of Cybersecurity Anthony J. Ferrante and Director Matt McManus discuss the current threat to the open Internet and the path to de-escalating global tensions in this *Security Magazine* article. Click to read.

THE DIGITAL OPERATIONAL RESILIENCE ACT: KEY QUESTIONS BUSINESS LEADERS SHOULD BE ASKING

The first draft of the 'Digital Operational Resilience Act' (DORA) was recently published by the European Commission. In this article, we assess the DORA proposal and outline the key questions business leaders should be asking. Click to read.

Follow us on LinkedIn to stay up to date on the latest news & events

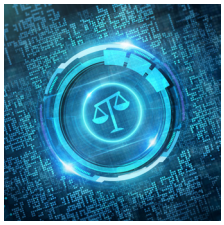
A LOOK BACK & AHEAD

RECENT EVENTS

INCIDENT RESPONSE FORUM RANSOMWARE 2021

January 14 | Virtual

Strategic Communications' Managing Director Meredith Griffanti participated in a panel discussion on Ransomware Before and After: Preparation and Remediation.



LEGAL RESOURCE NETWORK – BEFORE THE BREACH

January 27 | Virtual

Managing Director David Dunn delivered a keynote presentation on what law and accounting firms need to consider prior to suffering a cybersecurity breach.

A LOOK BACK & AHEAD (CONTINUED)

RECENT EVENTS (CONTINUED)

DATA PRIVACY DAY
January 28 | Global

Data Privacy Day is an international effort to empower individuals and encourage businesses to respect privacy, safeguard data, and enable trust. Click to learn more.

UPCOMING EVENTS

CYBERSECURITY BEST PRACTICES FOR LAWYERS 2021
February 1 | Virtual

Head of Cybersecurity for the Americas Jordan Rae Kelly will participate on a panel during Practising Law Institute's Cybersecurity Best Practices for Lawyers 2021 webcast program. Click to learn more.

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 FTI Cybersecurity. The Cybersecurity Briefing Book provides team and service offering updates, as well as trends that we are identifying that may affect your practices and clients. 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.