SERVICE SHEET

Cyber Incident Response Simulations

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

According to the 2021 FTI Resilience Barometer, for the third year in a row, the number of G20 organizations affected by cyber attacks has increased – up to 78%. Despite this increase, organizations often have outdated incident response plans, creating a disjointed approach to mitigating risk and combatting threats. A cyber incident response simulation (CIRS) is the ideal way to evaluate response efforts and understand strengths and weaknesses to improve an organization's effectiveness and efficiency during a cyber incident.

Benefits of a Cyber Incident Response Simulation

— Lessen the possibility of a cyber incident and minimize the potential impact when one occurs

— Evaluate existing response and preparedness capabilities in a hands-on, stress-free setting

— Instill confidence in internal teams and stakeholders by clarifying and practicing their specific roles

— Enhance the collective decision-making process throughout the incident response lifecycle

— Evaluate your organization's current incident response plan for effectiveness

— Assess available in-house and third-party resources to maximize their utilization

— Test and learn best practices for engaging with employees, customers, vendors, partners, media, regulators, law enforcement, and other key stakeholders

OUR DELIVERABLES

- A Cyber Incident Response Simulation tailored for your specific team participants; operational, senior leadership, or both; and designed around your organization's desired objectives
- Bespoke, plausible scenarios, developed around the current threat landscape, intended to challenge your organization's existing plans, processes, and team members
- Thorough review of existing incident response plan and policies
- Industry-specific cyber threat briefing highlighting recent incidents and evolving attack methods
- Ability to conduct simulation in-person or virtually
- After action report with recommendations for optimizing your crisis policies and processes, informed by real-world incident response best practices
- Improved clarity for the incident response team on how to appropriately execute the incident response plan during a cyber event
- Experienced facilitators with real-world cyber incident response and investigation experience

You Have an Incident; Now What?

To be crisis-ready and responsive, everyone must know their roles and responsibilities in advance. Waiting until an incident occurs to determine who does what is too late. Every second counts and lost time equals lost information, resources, reputation, or all of the above.

With an emphasis on training and learning, FTI Cybersecurity's preparedness planning services focus on developing best practice crisis management skills and knowledge. Considering unique qualities, we can design a cyber incident response simulation that best suits yours needs. FTI Cybersecurity will improve the various phases of an emerging crisis, discussing options and making consequential decisions at each juncture.

We Can Tailor a Program to Help Clients in Any Industry

What to Expect

Pre-Briefing

FTI Cybersecurity's CIRS team works with clients to understand their organization's operations and critical assets. We then design a custom cyber incident simulation, either discussion-based or operations-based, to evaluate an organization's response, injecting real-world movements. While each simulation is uniquely customized for each organization, here is an overview of what to expect for a half-day crisis simulation.

On the Simulation Day

A typical half-day incident response simulation includes:

- Session briefing and platform familiarization
- Live crisis simulation
- Exercise debrief, discussing lessons learned, successes, gaps, and the path forward

Post-Simulation

FTI Cybersecurity's experts deliver feedback and an in-depth report outlining your organization's strengths, gaps, recommendations for process, policy, and capability improvements.

Who Should Attend

All individuals who would be involved in managing the different aspects of a cyber incident.

Typically, this includes:

- C-Suite
- Senior Management
- General Counsel / Outside Counsel
- Chief Risk Officer
- Business Continuity Planning Teams
- IT and Information Cybersecurity Teams
- Communications, Media & Public Affairs Teams
- Board Members
- Customer Service Teams

CASE STUDY

Two-part Ransomware Simulation for a Critical Infrastructure Organization

SITUATION

FTI Cybersecurity was engaged to develop a two-part cyber incident response simulation designed specifically for the information technology team (part 1) and the executive leadership team (part 2) of a major municipal water supplier.

OUR ROLE

The FTI CIRS Team tested the participants with a custom-designed scenario that exposed the organization to the lifecycle of a ransomware incident affecting their organization and the critical response elements that should be considered.

OUR IMPACT

The two-part simulation allowed this critical infrastructure organization to assess the initial incident response procedures of their information technology team and then evaluate their executive leadership team as they explored best practices for internal and external communications and the overall information gathering and decision-making processes involved with a ransomware event.

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

1982

Year Founded and $5.4B equity market capitalization*

9/10

Advisor to 9 of the world's Top 10 bank holding companies

6,950+

Employees

NYSE:FCN

Publicly traded

98/100

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

59

59 of Fortune Global 100 corporations are clients

**Number of total shares outstanding as of April 21, 2022, times the closing share price as of April 28, 2022.*

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
Senior Managing Director
+1 267 507 2863
david.dunn@fticonsulting.com

MASON DREW
Managing Director, Cybersecurity
Singapore
+65 6506 9870
mason.drew@fticonsulting.com

EVAN ROBERTS
Managing Director, Crisis Comms
New York
+1 212 850 5777
evan.roberts@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. FTI Consulting, Inc., including its subsidiaries and affiliates, is a consulting firm and is not a certified public accounting firm or a law firm. ©2022 FTI Consulting, Inc. All rights reserved. **www.fticonsulting.com**