FTI CONSULTING | CYBERSECURITY

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

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 300 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?

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.

Real-world Scenarios

FTI Cybersecurity's Preparedness Planning team offers custom crisis exercises and evaluations designed to test and improve an organization's incident response capabilities. How companies react to and communicate about cybersecurity incidents is critical, and there is only one chance to get it right. Our integrated team of cybersecurity and crisis communications experts helps companies do just that.

The aim is to replicate the operational and communications challenges of a cyber incident through realistic pivot-points and roleplay. Using real-world scenarios and simulations, we help clients understand their threat profile, prepare a response plan, understand their weak points, and harden their defenses.

With an emphasis on training and learning, FTI Cybersecurity's Preparedness Planning services focus on developing best practice crisis management skills and knowledge. Considering your organization's unique qualities, we can design a program that best suits your needs. From seminars and table-top exercises to full-scale crisis simulations, FTI Cybersecurity will improve any organization's ability to address the various phases of an emerging crisis, discussing options and making consequential decisions at each juncture.

Intelligence-led, Expert-driven

FTI Cybersecurity's Preparedness Planning team is led by cybersecurity and crisis management experts with decades of experience at the highest levels of government, law enforcement, and global private sector institutions. Our team will observe how the organization responds and handles the incident – evaluating both executive strategy and technical action – while gathering feedback to help create a more efficient process flow.

We can tailor a program to help clients in any industry

Benefits

- *Highlight strengths and identify vulnerabilities in your organization's existing crisis processes, structures, and skills*
- *Evaluate your organization's incident response plan for effectiveness*
- *Simulate the tactics, techniques, and procedures of real-world threat actors that target your industry*
- *Test your organization's ability to respond to regulatory requirements in proper timeframes*
- *Learn how to effectively engage with outside parties that may be involved in an incident or impacted by an incident*
- *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*

Who Should Attend

All individuals who would be involved in managing a crisis. Typically, this includes:

- C-Suite
- Board Members
- Senior Management
- Chief Risk Officer
- General Counsel
- Business Continuity Planning Teams
- Technical Leaders
- Communications, Media & Public Affairs Teams
- Customer Service Teams

What to Expect

Pre-Briefing

FTI Cybersecurity's Preparedness Planning team works with clients to understand their organization's operations and critical assets. We then design a custom exercise, 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 Crisis Simulation Day

A typical half-day crisis simulation exercise includes:

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

Post-Crisis Simulation

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

Anthony J. Ferrante
Global Head of Cybersecurity
Senior Managing Director
+1 202 312 9165
ajf@fticonsulting.com

Brian Kennedy
Head of the Americas,
Strategic Communications
Senior Managing Director
+1 202 346 8826
brian.kennedy@fticonsulting.com