Cybersecurity Business Continuity Services

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

Cyber attacks have the potential for devastating consequences, including loss of revenue and customer confidence, damaged reputation, and costly remediation efforts, in addition to impeding your ability to keep your business up and running. Preventing these debilitating results, and ensuring that operations do not stall, requires a business continuity and disaster recovery plan.

Could Your Organization Survive a Cyber Attack?

Cyber attacks are often designed to compromise all versions of data including backups. Would your organization be capable of continuing to operate if critical data was destroyed? What about attacks that hinder normal business functions like a distributed denial-of-service (DDoS) attack or ransomware? Being able to combat the full range of cyber threats requires a proper business continuity plan that has been implemented and tested in advance.

Business Continuity Management

Business Continuity Management (BCM) involves a comprehensive process of threat identification, specific to your organization, and the potential business operations impact that those threats carry. From there, a resiliency framework can be established that defines response protocols. Once the assessment and creation of the BCM program is implemented, it should be tested and altered based on results. It is an ongoing process that requires complete organizational buy-in. Don't waste time developing a plan during a disaster – every second counts.

Achieve Cyber Resilience

The goal of any business continuity plan should be to achieve cyber resilience. Cyber incidents are inevitable and being able to maintain normal operations even while under attack is critical. The risks of not implementing proper protocols in advance are too costly. Maintaining revenue flow, upholding your reputation, preserving customer and stakeholder confidence, and preventing the need for remediation are all otherwise at stake.

Effective Crisis Communications

Effective internal and external communication is crucial during any cybersecurity incident. When the stakes are high, it is imperative to know what to say, how and when to say it, and to whom. Cyber attacks often involve legal, financial, regulatory, and reputational implications – all of which can be damaged without proper communications to all involved parties (*i.e.* customers & partners, shareholders, third parties, lawmakers & regulators, employees, media).

Why FTI Cybersecurity

Multidisciplinary Expertise

Intelligence-led, expert-driven, strategic approach to cybersecurity challenges

Core team from intelligence agencies, law enforcement, prosecuting offices, 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 $4.9B equity market capitalization*

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

7,500+
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 October 20, 2022, by the closing price per share on October 27, 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 & APAC
Senior Managing Director
+44 7816 251410
david.dunn@fticonsulting.com

FTI CONSULTING™