Subject: **FTI Cybersecurity Briefing - August 2026**
From Name: **FTI Cybersecurity**
From Email: **no-reply@info.fticonsulting.com**
Reply-to Email: **#CYBERSECURITY-ACTION@fticonsulting.com**
Preview Text: **What's Inside: Cyber Attacks Target Financial Industries and the U.S. Water Systems, CMMC Updates, and More!**

FTI CONSULTING | CYBERSECURITY

View in Browser

What's Trending

U.S. water and wastewater systems are facing growing cyber threats as attackers increasingly target the operational technology (OT) that controls critical infrastructure. Recent activity highlights the vulnerabilities of internet-connected systems and the potential for cyber incidents to disrupt essential services, underscoring the need for utilities to strengthen OT security, improve network visibility, and build resilience against evolving threats. **Read More >>**

Cyber Attacks Target Major Wall Street Firms
Major Wall Street financial firms and money managers have been targeted in a series of sophisticated cyber attack attempts, with hackers using social engineering and phone-based tactics to trick employees into providing access to systems or sensitive information. The attacks highlight the continued effectiveness of human-focused techniques and the need for financial institutions to strengthen defenses against evolving cyber threats. **Read More >>**

Service Spotlight

Why It Matters:
The Department of War's (DOW) suspension of CMMC Phase II changes how compliance is verified, not whether it's required. All 110 NIST SP 800-171 controls, incident reporting obligations, and SPRS score submissions remain mandatory. An inaccurate SPRS score can trigger False Claims Act liability, and non-compliance risks withheld payments, stop-work orders, or debarment. With third-party certification potentially returning in a new form, organizations that let their security posture slip now will face a steeper and more costly path to compliance later.

How FTI Consulting Can Help:
FTI Consulting helps defense contractors stay compliant through regulatory uncertainty. Our team, with backgrounds in intelligence, law enforcement, and the private sector, conducts defensible NIST SP 800-171 assessments, calculates accurate SPRS scores, and develops key compliance artifacts, including SSPs, POA&Ms, and incident reporting procedures. We also advise on subcontractor flow-down, cloud security, and gap remediation.

Success Story:
A U.S. drone software company needed CMMC compliance to become a government vendor. FTI Cybersecurity conducted a NIST SP 800-171 readiness assessment, developed an SSP and POA&M, and remediated gaps including mobile device management and access controls. The company's NIST score improved significantly, positioning it for CMMC certification.

Learn More About Our CMMC Update Services

In the News

In this *ITPro* article, **Adam Harrison** shares his views on the importance of rapid response and containment after a cyber attack. **Read More >>**

In this *TechTarget* article, **Matt McClelland** explains how organizations can use a data mesh to support AI initiatives while addressing the governance, skills, and organizational challenges that can hinder adoption. **Read More >>**

In this *Digital Health Insights* article, **Jamie Singer** notes that most cyber attacks she has observed targeting medical technology companies involve data access and extortion. **Read More >>**

Expert Perspectives

In this article, **Keith Swiat** discusses the importance of private equity firms embedding cybersecurity into the full hold period because, at exit, buyers now price cyber risk directly into their offers. **Read More >>**

In this article, **Elizabeth Kwok** and **Ryan Smyth** share how to move beyond written policies to proving controls work as designed to comply with the new CCPA cybersecurity audit regulations. **Read More >>**

In this article, **Breck Heidlberg** explains that ICTS compliance becomes an operational imperative and outlines how to build proactive programs to manage national security risks in supply chains. **Read More >>**

In this article, **Paul Abbate** explores how public-private partnerships are evolving to address emerging national security risks. *Please note that this article requires a subscription.* **Read More >>**

In this article, **David Manek, Joe Knight, Colleen Yushchak, Kenric Tom,** and **Chris Zohlen** discuss how AI regulations are reshaping privacy rights governance. Learn how CCPA and other emerging AI laws impact your organization's compliance roadmap. **Read More >>**

In this article, **Matt McClelland** and **Matt Flora** share the 5 most common HIPAA security risk analysis findings and how organizations can effectively address compliance gaps. **Read More >>**

In this article, **Carlos Araujo Jr.** and **Antonio Gesteira** write that, in the event of a cyber incident, a dangerous mismatch exists between perception and reality in Brazilian organizations' response capabilities. **Read More >>**

View All Insights

Upcoming Events

September 10 AMERICAS	**Financial Infrastructure and Innovation Summit - Risk, Controls, AML, Fraud, Cyber, and Financial Crime Readiness**	**Mike Driscoll** **Alma Angotti**

Have an Incident?

Email #FTICYBERSECURITY-RESPONSE@fticonsulting.com or call one of our response lines.

Was this email forwarded to you? Interested in more monthly cybersecurity insights?
Subscribe to the FTI Cybersecurity Briefing below!

Subscribe

FTI CONSULTING