NEW WHITE PAPER CALLS FOR EXPANDING CROSS-INDUSTRY COORDINATION TO MITIGATE THE SYSTEMIC IMPACT OF A MAJOR CYBER ATTACK ON THE FINANCIAL SYSTEM

More than 50 experts cite collective response & recovery plan and contingent arrangements as top priorities

New York/London/Hong Kong/Singapore/Sydney, March 20 2018 – As cyber-threats against the financial sector become more frequent, complex and sophisticated, cross-industry coordination around response and recovery mechanisms are essential to mitigating the systemic consequences of a large-scale attack, according to a white paper published today by The Depository Trust & Clearing Corporation (DTCC), the premier post-trade market infrastructure for the global financial services industry, and Oliver Wyman, a leading global management consulting firm.

The white paper cites a need for additional efforts around specific cyber-scenarios and limited industry-wide testing as two key factors that could complicate the ability of banks and other financial institutions to react quickly to an attack.

The paper, which features extensive research and interviews with over 50 subject matter experts including financial services and non-financial services practitioners, recommends increased coordination across the industry, the development and implementation of standards to facilitate effective response and recovery and adherence to regulatory principles. Two key initiatives are suggested:

- **Developing a collective response & recovery plan, outlining key response and recovery requirements:** The industry currently lacks standards around key considerations, including the definition of resumption and recovery; the criteria for safe resumption of operations; the appropriate timeframes for resumption and recovery; and plans for communicating with the public during a large-scale cyber-attack. The proposed initiative would identify collective actions to be taken upon the detection of a large-scale cyber-attack, based on a set of standardized criteria that is tailored to specific cyber-attack scenarios. Results would be included in industry playbooks.

- **Establishing contingent service arrangements:** Given the complexity and broad scope of large-scale cyber-attacks, no single entity has all the required capabilities to address every possible attack and vulnerability. Regardless of the level of preparedness, there may be situations where a critical provider is unable to fulfill its services for an extended period, creating the
need for contingent service arrangements. This initiative would explore arrangements to enable firms to continue critical operations if they or a partner suffer an outage from a cyber-attack.

Commenting on the ever-growing threats to the industry, Andrew Gray, Chief Risk Officer at DTCC, stated, “An attack on one or more institutions or critical infrastructures could have a contagion effect across the financial system, especially as interconnectedness continues to grow. As a result, it is critically important that firms incorporate additional redundancies to ensure that the failure of any single institution can be contained and mitigated. To successfully achieve this, we must collectively prioritize resilience and recovery efforts across market participants, infrastructure providers, technology vendors and regulators.”

Commenting on the need for further coordination, Paul Mee, Partner, Digital and Financial Services, Cyber Platform Lead at Oliver Wyman, stated, “Mitigating the systemic consequences of the increasing threat of large-scale cyber-attacks on the financial system is matter of national and international security. In what is arguably a global cyber arms race, it is clear that major players need to be prepared, connected and coordinated in order to effectively respond to and rapidly recover from a large-scale cyber-attack.”

To move these efforts forward, the paper suggests identifying initiative owners, key stakeholders and responsibilities, as well as the further exploration of specific objectives and implementation plans.

# # #

About DTCC
With 45 years of experience, DTCC is the premier post-trade market infrastructure for the global financial services industry. From operating facilities, data centers and offices in 16 countries, DTCC, through its subsidiaries, automates, centralizes and standardizes the processing of financial transactions, mitigating risk, increasing transparency and driving efficiency for thousands of broker/dealers, custodian banks and asset managers. Industry owned and governed, the firm simplifies the complexities of clearing, settlement, asset servicing, data management and information services across asset classes, bringing increased security and soundness to financial markets. In 2016, DTCC’s subsidiaries processed securities transactions valued at more than U.S. $1.5 quadrillion. Its depository provides custody and asset servicing for securities issues from over 130 countries and territories valued at U.S. $49.2 trillion. DTCC’s Global Trade Repository maintains approximately 40 million open OTC positions per week and processes over one billion messages per month.

About Oliver Wyman
Oliver Wyman is a global leader in management consulting. With offices in 50+ cities across nearly 30 countries, Oliver Wyman combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation. The firm has more than 4,700 professionals around the world who help clients optimize their business, improve their operations and risk profile, and accelerate their organizational performance to seize the most attractive opportunities. Oliver Wyman is a wholly owned subsidiary of Marsh & McLennan Companies [NYSE: MMC]. For more information, visit www.oliverwyman.com. Follow Oliver Wyman on Twitter @OliverWyman