Crowell

CLIENT ALERT

The DAO Hack Provides Lessons for Companies Using Blockchain and Distributed Ledger Technology

June 27, 2016

The Decentralized Autonomous Organization (the DAO), an anonymous, crowd-sourced investment vehicle using the digital currency Ether, was recently hacked in a heist that saw investors lose 3.6 million Ether coins valued at $55 million. Prior to the hack, the DAO was notable as one of the first investment funds operating on the Ethereum blockchain, a distributed ledger technology supporting "Ether" digital currency. Some news media have gone so far as to predict the end of virtual currencies in the wake of this incident. However, the incident can be taken instead for the important lessons it provides, and to inform cybersecurity readiness for safer deployment and adoption of blockchain and distributed ledger technologies.

By way of background, Ether is a digital currency similar to Bitcoin, and is traded through the Ethereum blockchain. Unlike Bitcoin, Ethereum supports "smart contracts"—automated computer programs that execute the terms of a negotiated contract.

The DAO operated using smart contracts built on the Ethereum blockchain. When investors transferred their Ether to the DAO pool, the DAO smart contract enabled these investors to vote on how the pool would be invested. The smart contract also contained an automated mechanism to enable investors to exit from the DAO that, when executed, told the DAO where to distribute their Ether. Unknown hackers exploited a weakness in the code of DAO's smart contract, enabling them to withdraw not only the Ether hackers placed in the DAO, but also the Ether of other investors.

Importantly, the DAO hack was not caused by any inherent weakness in blockchain or distributed ledger technologies; it was specific to DAO. However, the incident demonstrates the importance of cybersecurity readiness, including timely threat assessment and organizational response. The DAO hack was perpetrated by exploiting a flaw in DAO's smart contract code—a vulnerability that was publicly identified in May, well ahead of the attack.

Traditional investment vehicles such as mutual funds and commodity pools are incentivized by the threat of civil liability and regulatory penalties to continuously test their systems. Regulators have made it clear that financial intermediaries such as fund managers, commodity pool operators and investment advisers must take care to ensure that their clients' assets and information are protected. The Securities Exchange Commission's (SEC's) February 2015 Cybersecurity Alert is one example, and the National Futures Association's August 2015 Guidance is another. Regulators have also made it clear that investment activities involving virtual currencies can have real-world repercussions. The Commodity Futures Trading Commission has asserted jurisdiction over virtual currencies as commodities, most recently in an order requiring Bitcoin exchange Bitfinex to register as a Futures Commission Merchant, and the SEC has made it clear that regardless of whether a securities investment is paid for in virtual or fiat currency, it is still subject to the agency's jurisdiction.

Unlike traditional financial intermediaries, the DAO does not appear to fall into any category of regulated entity. As its name implies, the DAO is autonomous—it is self-executing computer code. And although one or more individuals created the DAO's code, it is not clear whether those individuals will ever be identified or will continue their involvement. Thus, there may be no investment adviser, commodity pool operator or other regulated entity to take responsibility for maintaining the DAO's security.

The DAO's code is open source, and therefore open to the public to identify and fix vulnerabilities and to make other changes. However, simply because the code is open source does not mean that anyone will necessarily take on the responsibility to identify and fix vulnerabilities much less take on liability for failing to fix known flaws. Given the anonymous and distributed nature of the DAO, there is little, if any, incentive to undertake the cybersecurity measure typically implemented by more traditional financial intermediaries.

As the DAO hack demonstrates, all firms using distributed ledger technologies or virtual currencies need to ensure that their own applications, as well as those they engage with, employ best practices for cybersecurity. Not only should firms prepare for incident response and crisis management in advance, but also proactively review their policies and procedures, system controls, and vendor management practices. Cyber risk review—including accessing threat intelligence and participating in Information Sharing and Analysis Organizations (ISAOs), as appropriate—and timely organizational response should be ongoing activities.

Cybersecurity has become one of the most important issues for companies and a critical consideration for managing risk, especially when incorporating new technologies. Crowell & Moring's depth of experience enables us to inform clients about emerging cybersecurity and privacy issues and risks and provide proactive counseling in assimilating new cyber/privacy requirements and new technologies like blockchain into existing business frameworks.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Evan D. Wolff
Partner – Washington, D.C.
Phone: +1 202.624.2615
Email: ewolff@crowell.com

Matthew B. Welling
Partner – Washington, D.C.
Phone: +1 202.624.2588
Email: mwelling@crowell.com