



Elizabeth P. Gray Partner
egray@willkie.com

Katherine Doty Hanniford Associate
khanniford@willkie.com

Willkie Farr & Gallagher LLP, Washington, DC

Cyber risks and short selling: new threats in the digital health space

In autumn 2016, US medical device company St. Jude Medical filed suit against hedge fund Muddy Waters and research firm MedSec Holdings, claiming that the latter pair of companies had aimed to impact St. Jude's stock rating through their claims about alleged cyber security vulnerabilities in certain of St. Jude's products. It is reported that Muddy Waters had taken a short position in St. Jude's, and thus some commentators are viewing the situation as an example of a new trend in the cyber security arena, in which short selling firms stand to profit after releasing information about firms' cyber vulnerabilities. Elizabeth P. Gray and Katherine Doty Hanniford of Willkie Farr & Gallagher LLP discuss the implications of such trends in the wider context of evolving cyber threats and their impact on public companies.

The emergence of cyber security as a critical component of risk management and corporate governance has been underway for some time, but recent attacks such as the ransomware attacks on healthcare systems in the first quarter of 2016 and the massive and sustained botnet attack in the fourth quarter of 2016 have brought cyber security to the forefront of corporate risk assessment. While financial regulators have increased their focus on cyber security, these attacks demonstrate both the interdependency of the digital economy and how unsuspecting consumers and unprepared companies alike can be put at serious risk. While some market research has noted that most consumers expect companies to be hacked - that the question is no longer whether but when - it is hard to overstate the reputational and legal risks to companies that experience cyber events.

Evolving cyber threats and their impact on public companies

While some participants in the digital economy correctly view cyber security as capable of posing an existential threat to enterprise risk management, others have been slower to recognise and adapt to the threat. In conjunction with this cyber readiness gap, there are some market participants that have seized upon the disruption and uneven or insufficient risk management to craft investment strategies. One widely reported example of this has been hedge fund Muddy Waters' partnership with research firm MedSec¹. Together, the two entities have been critical of St. Jude Medical, Inc. for alleged cyber security flaws in its pacemakers. Rather than take concerns of potential cyber security vulnerabilities to St. Jude Medical, Muddy Waters reportedly took a short position in St. Jude and publicly released a research report. It has been reported that MedSec did not go to the company with its concerns because it was "worried that [St. Jude] would sweep

this under the rug²." St. Jude is in the process of being acquired by Abbott Laboratories, and in September 2016 sued Muddy Waters for defamation³. In January 2017, the U.S. Food and Drug Administration issued a safety communication in which it identified cyber security vulnerabilities in St. Jude pacemakers⁴.

These developments pose foundational questions for the role of consumer protection and shareholder activism in the digital era. Part of what distinguishes this example from the usual instances of hedge fund criticism of corporate practices is that the allegations highlight cyber security risks that could be fatal, and go well beyond the usual downside risk of loss of capital, marketshare, or reputation⁵. The alleged cyber security flaw at St. Jude Medical pertains to pacemakers, which if hacked could conceivably cause serious health side effects or death. Thus, there are compelling reasons why research analysts or consumer advocates would be interested in blowing the whistle on a company whose consumer devices are shown to be unreasonably susceptible to cyber attack or whose management is perceived as being lax or slow to recognise cyber security as a core corporate governance principle, on par with a robust audit committee, for example.

While Muddy Waters and MedSec have positioned themselves in the press as consumer protection advocates, there is the potential for serious risks stemming from their short position in St. Jude. Irrespective of the merits of arguments such as (i) Muddy Waters and MedSec did not want to share the information with St. Jude because they viewed St. Jude as having downplayed cyber security risk, or (ii) hedge funds and research outfits are entitled to profit from identifying cyber security flaws, securities regulators may be more interested in Muddy Waters' short positions and the timing of its trades.

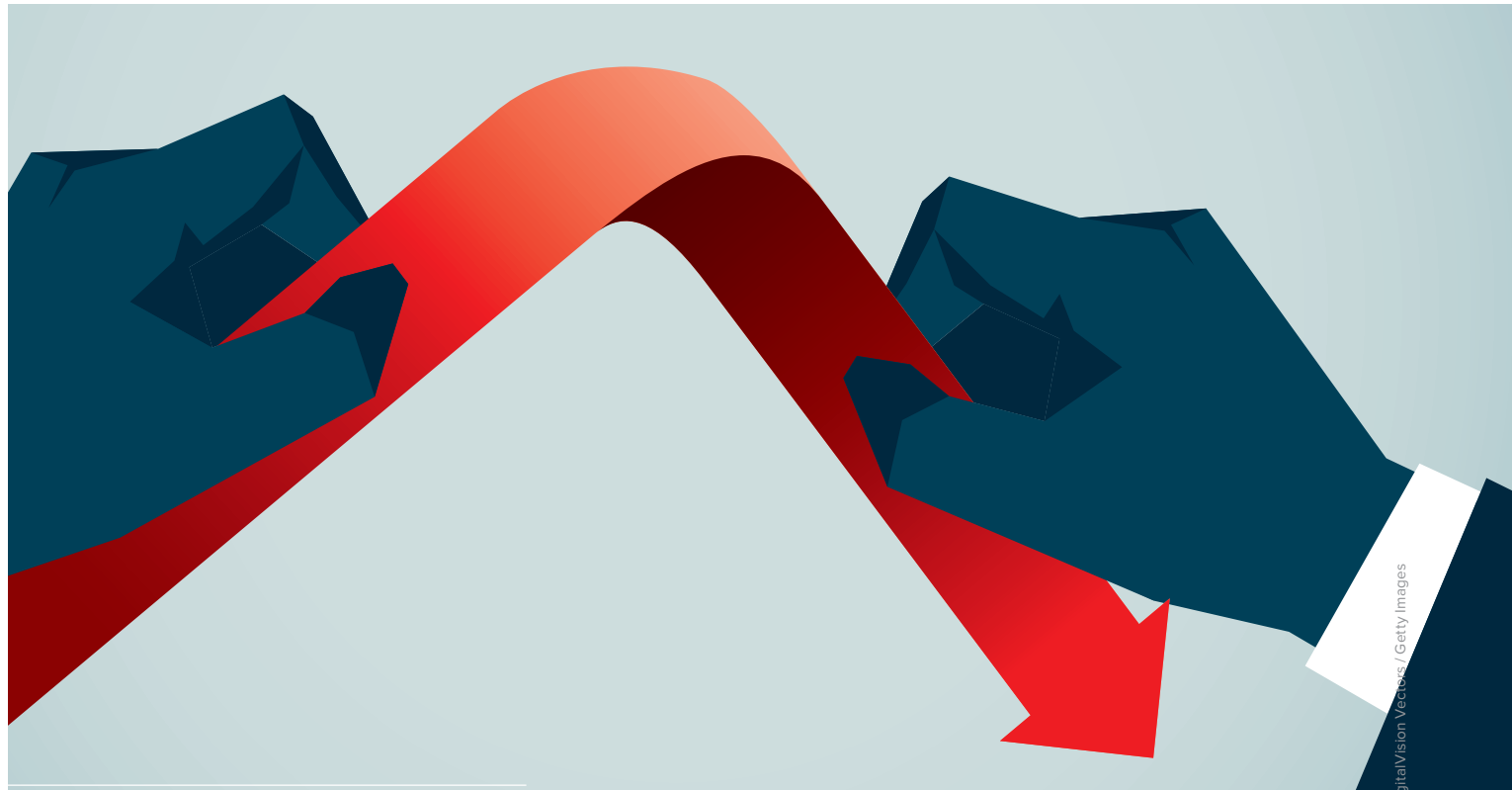


Image: erhuiz9 / DigitalVision Vectors / Getty Images

While Muddy Waters and MedSec have positioned themselves in the press as consumer protection advocates, there is the potential for serious risks stemming from their short position in St. Jude.

Hedge funds should consider the risk that their short selling actions may be viewed by regulators as market manipulation, once the fund (or an affiliated research arm) makes public statements about a target stock that could be interpreted as artificially designed to depress stock price.

By contrast, if a hedge fund identifies an issuer as especially vulnerable to cyber attack, and decides to short it, without publicising its findings, there is no conflict. The hedge fund is under no obligation to inform the issuer, but it also has no additional edge to the short since it has not induced a cyber attack, and since it is unclear whether the issuer would publicly disclose a cyber attack, two actions that increase the likelihood that the issuer's share price will decrease. In order for this second trading strategy to work, a cyber attack must be viewed as material information that the issuer is obligated to publicly disclose under the US Securities and Exchange Commission ("SEC") regulations and common law. This seems appropriate, particularly in light of the severe consequences to consumers that can result from cyber attacks. Issuers and boards should be pursuing robust cyber risk governance and management practices, investors should be aware of those outliers that are not engaging in best practices. Public companies must heed the call to institute robust cyber risk management processes, and involve the most senior level of governance, the Board of Directors and C-suites.

Cyber security risk also may affect the push for an informational advantage that informs a short position. In gathering information to develop a trading theory, a firm may be tempted to mine the dark web for information regarding a target issuer. Here, too, a firm could run into market manipulation risks. Informational advantages gleaned from the dark web may be

gained through material non-public information ("MNPI"). Such MNPI may be offered for sale on the dark web by someone who owes a duty to the company; should a firm pay for such information, it may run afoul of US federal insider trading law.

Public companies, too, should be concerned about the spread of corporate information - whether true or false - on the dark web and its use in trading strategies. The availability of material corporate information on the dark web implicates the semi-strong efficient market hypothesis, an economic theory that undergirds the judicial review of stock price, reliance, and loss causation in securities fraud actions⁶. The semi-strong efficient market hypothesis posits that prices reflect all publicly available information and adapt quickly to factor that information into pricing⁷. If material corporate information is for sale on the dark web, it is not necessarily limited in its distribution as in a classic insider trading case, but rather may be passed to multiple parties by the tipper or tippees. If market participants are basing trading positions on information gleaned from the dark web, that dark web information begins to affect the price of the underlying security.

Corporate governance implications

The rise of cyber security threats like the ones discussed above poses serious corporate governance challenges to boards and management alike. Fortunately, there are steps that SEC registrants can take to protect themselves against cyber attacks. First, boards should treat cyber security risk management as a critical corporate governance issue. Similar to the board's approach to audit integrity, a critical number of individual board members should have cyber security expertise or, at a minimum, access to independent personnel with the expertise to address cyber security

Strong policy reasons remain for regulatory scrutiny of cyber security risk management and any perceived inducements to attack a company for its suspected weaknesses in cyber readiness.

continued


issues. Second, in conjunction with assessing an entity's enterprise-wide cyber security issues, the board should re-examine reporting lines and responsibilities that touch on cyber security risk management to ensure appropriate communication, accountability, and risk management. Boards that continue to treat cyber security as merely an extension of existing information security programs and governance do so at their peril. Rather, boards should direct a cyber security risk assessment in order to identify the entity's assets and associated threats on an enterprise-wide basis. In order to preserve the confidentiality of this process, boards should engage outside counsel to direct the assessment. In conjunction with this assessment, entities should consider contracting with a third party consultant to safely and anonymously access the dark web to ascertain what information may be available about the entity on the dark web and whether the entity has already been subject to a data breach. As a result of this assessment, the entity should develop and implement comprehensive cyber security policies and procedures, which they should test periodically. Boards should ensure that such testing includes penetration testing, or white hat/black hat exercises, and that such testing is comprehensive enough to challenge the entity's crisis management response capabilities and the strength of its cyber security rulebook.

In addition to enhancing a company's cyber security preparedness, the assessment process will also provide the board with essential risk governance information, including what specific threats face the company, whether management is equipped and prepared to handle cyber security risk management and response, and other legal and regulatory considerations that are specific to the company, including reporting obligations and information sharing. For example, some market sectors may take advantage of existing safe

harbors for information sharing related to cyber security that protect them from antitrust and other legal liability that would otherwise result from such coordination⁸. Counsel can assist the board in navigating which safe harbors and other information sharing opportunities may be available and when reporting obligations may be triggered.

Boards also should consider implementing an internal whistleblower and external bounty program to hold the issuer accountable for the cyber security integrity of its operations, products, and services but reduce the likelihood of a publicity-driven cyber attack.

The SEC has offered guidance on cyber security risk disclosures⁹. It expects registrants to disclose cyber security risks that are significant and material to the entity, and to do so in a specific and informative fashion that avoids boilerplate or generic disclosure. However, the SEC also recognises registrants' needs to maintain certain information as confidential precisely due to security risks. Therefore, SEC registrants must balance the need for meaningful disclosure of material cyber security related risks with the need to protect themselves and avoid compromising their own cyber security. Here, too, St. Jude Medical provides a case in point. Beginning in 2015, St. Jude Medical included disclosure of cyber security risk as one of the most significant risk factors that could affect future operations¹⁰. Its 2014 and 2015 Forms 10-K and 2015 Forms 10-Q contain language that identifies cyber security as a risk and, to varying degrees, discusses that risk. Following the allegations by MedSec and Muddy Waters, and amid an investigation into those allegations by the Food and Drug Administration, St. Jude formed a medical advisory board to focus on cyber security issues relating to patient care and safety¹¹. It remains unknown whether St. Jude

- 
1. See, e.g., Matthew Goldstein, Alexandra Stevenson, Leslie Picker, 'Hedge Fund and Cybersecurity Firm Team Up to Short-Sell Device Maker,' *New York Times*, 8 Sept 2016.
 2. *Ibid.*
 3. *St. Jude Medical, Inc. v. Muddy Waters, MedSec Holdings et al.*, D. Minn., Case No. 16-cv-03002 (filed 7 Sept 2016).
 4. FDA Safety Communication, *Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter*, 9 Jan 2017; available at <http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm>
 5. The healthcare sector appears to be especially vulnerable to cyber security risk given the concentration of information (financial payments, insurance, and private medical information) and the array of systems and devices that would need to be patched on a timely basis. Nevertheless, the healthcare sector may also have at least one natural defence: its systems and devices may be unique or not well-integrated, so hacking into one does not necessarily lead to a comprehensive breach, and can instead be detected and well protected using a multi-layer defence strategy.
 6. *Basic v. Levinson*, 485 U.S. 224 (1988). '[I]n an open and developed securities market, the price of a company's stock is determined by the available material information regarding the company and its business.'
 7. Eugene Fama, 'Efficient Capital Markets: A Review of Theory and Empirical Work,' *Journal of Finance*, Vol. 25, Issue 2, May 1970.
 8. See, e.g., USA PATRIOT Act Section 314(b).
 9. U.S. Securities & Exchange Commission, Division of Corporation Finance, *CF Disclosure Guidance: Topic No. 2 Cybersecurity* (13 Oct 2011), available at <https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>; U.S. Securities & Exchange Commission, Division of Investment Management, *Cybersecurity Guidance*, Apr 2015, No. 2015-02, available at <https://www.sec.gov/investment/im-guidance-2015-02.pdf>
 10. See, e.g., *St. Jude Medical, Inc.* Form 10-Q (filed 4 May 2016).
 11. Reuters, 'St. Jude Medical Will Form a Cybersecurity Board After Heart Device Defect,' 17 October 2016, available at <http://fortune.com/2016/10/17/st-jude-cybersecurity/>

Medical has taken additional steps beyond the formation of an advisory board but it is plausible that additional steps have been taken and are being maintained in confidence given the security concerns, irrespective of whether a reasonable investor would consider such information material.

Public policy considerations

Strong policy reasons remain for regulatory scrutiny of cyber security risk management and any perceived inducements to attack a company for its suspected weaknesses in cyber readiness. The troubling conduct here is the extent to which firms that might engage in vocal short selling based on negative cyber readiness assessments of a target could be viewed as effectively inducing a cyber attack on a target issuer. There are basic public policy reasons for prosecuting the inducement of a cyber attack on providers of medical services or products, and key infrastructure such as payments processing or telecommunications.

The harsh consequences of a cyber attack are also why many companies offer bounty programs that compensate people for bringing cyber security weaknesses to the company's attention in a non-public, confidential fashion so that the weaknesses can be resolved while minimising the risk of cyber attack in the meantime. Companies bear a significant responsibility to ensure they respond appropriately to such cyber security weaknesses when they are brought to their attention.

Weaknesses in those sectors' cyber readiness is also a public policy concern precisely because of the serious consequences that can result from cyber attack. Long has there been a role for consumer safety research, and this cyber security iteration of consumer safety research is not, in and of itself, a bad thing. Quite the opposite. The issue

here is the conflict of interest that arises where a research firm or a hedge fund identifies a critical safety flaw, publicises it, and then takes a financial position where its interests are aligned, and stands to benefit from criminal hacking activity. Once the firm takes a short position, it is no longer aligned with the so-called public interest of consumer safety and protection that it originally sought to publicise, because its financial position will only be advantaged should the issuer come under cyber attack, the basis for which it publicised.

For its part, US Congress could consider updating the Computer Fraud and Abuse Act, which penalises some hacking conduct, to better address current cyber attacks, and also consider the role that consumer safety research plays in the cyber security context. In this regard, too, the US Department of Justice could increase enforcement of the Computer Fraud and Abuse Act. It would be useful for the US Government to provide clarity as to the distinction between consumer safety research and nefarious behaviour.

If the incoming Republican Administration jettisons the broken windows approach to enforcement of the financial sector in favour of a return to first principles - sunlight as the best disinfectant - then SEC registrants should be especially careful to renew their attention to complete and accurate disclosure, including that of cyber attacks and cyber security weaknesses, and to the implementation of robust cyber security programs. It remains unclear whether and which regulators will continue with proposed rulemaking to strengthen cyber readiness across the digital economy, and to what extent regulations already in effect will be enforced. Despite the absence of regulatory clarity, SEC registrants must still maximise their cyber security risk governance framework in order to effectively defend against constantly evolving cyber threats.